Cybersecurity –

Ein Blick auf den Status quo bei Unternehmen in Deutschland

TeamViewer

Handelsblatt
RESEARCH INSTITUTE

Die Digitalisierung von Wirtschaft und Gesellschaft schreitet kontinuierlich voran. Unternehmen, Bürgerinnen und Bürger – aber auch öffentliche Einrichtungen – werden immer vernetzter und nutzen für ihr tägliches Handeln elektronische Daten oder digitale Kanäle.

Mit voranschreitender Digitalisierung werden auf der einen Seite die damit einhergehenden Vorteile und wirtschaftlichen Potenziale größer. Auf der anderen Seite wächst allerdings das Risiko für Cyberangriffe. Unabhängig von Branche und Unternehmensgröße sollte das Thema Cybersicherheit ganz oben auf der Liste der Themen stehen, mit denen sich Unternehmen intensiv beschäftigen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beurteilt die IT-Sicherheitslage im jüngsten Lagereport vom September 2021 als „angespannt bis kritisch". Die Angreifer werden immer erfindungsreicher und die Anzahl der Schadsoftware-Varianten steigt stetig. Zugleich nimmt die Qualität der Angriffe zu.

Solche Angriffe verursachen große Schäden, die in die Milliarden gehen können. Dies verdeutlichen Beispiele aus den Jahren 2016 und 2017, in denen es verstärkt zu Angriffen mit den Schadprogrammen WannaCry und NotPetya kam. Der globale Schaden durch WannaCry betrug laut BSI einige hundert Millionen bis zu vier Milliarden US-Dollar. Constanze Kurz, Sprecherin des Chaos Computer Clubs, bezifferte den Schaden sogar auf 4,5 Milliarden US-Dollar.

Noch größer waren die Auswirkungen durch NotPetya. Hier beliefen sich die weltweiten Schäden laut Peter Hacker, ein Experte und Berater für Cybersecurity, im Jahr 2017 auf rund 10 Milliarden US-Dollar. Allein bei den Logistikunternehmen Fedex und Maersk verursachte der Angriff nach Unternehmensangaben jeweils Kosten in Höhe von ungefähr 300 Millionen US-Dollar. So mussten bei Maersk 4.000 Server, 45.000 Computer und 2.500 Applikationen reinstalliert werden.

Auch in jüngster Zeit verdeutlichen Beispiele die Vulnerabilität der Unternehmen. Im März 2021 wurden Schwachstellen im Groupware- und E-Mail-Server Exchange von Microsoft bekannt, die zu dem Zeitpunkt durch ein außerplanmäßiges Sicherheitsupdate behoben wurden. Bis dahin hätten Angreifer Schadsoftware über die Schwachstellen in die Systeme einschleusen können. Da Exchange vielfach verwendet wird, waren bis zum Zeitpunkt des Bekanntwerdens der Schwachstelle laut BSI 98 Prozent der geprüften Systeme in Deutschland verwundbar.

Eine noch größere Dimension weist die Schwachstelle bei log4j auf, die im Dezember 2021 bekannt wurde. Dabei handelt es sich um eine Protokollierungsbibliothek für Java-Anwendungen. Durch diese Schwachstelle haben Angreifer ebenfalls Zugriff auf die Systeme. Die Herausforderungen bestanden darin, die Systeme wieder schnell zu sichern, ohne genau zu wissen, wo log4j überall im Einsatz ist. Das BSI stufte den Fall als „extrem kritisch" ein, in dessen Verlauf der Ausfall vieler Dienste sowie des Regelbetriebs nicht ausgeschlossen werden kann.

In zahlreichen Unternehmen haben die Cybersicherheits-Expertinnen und -Experten im Anschluss an das Bekanntwerden viele Überstunden gemacht.

Das log4j-Beispiel verdeutlicht, dass das Risiko nicht immer allein im direkten Verantwortungsbereich der Unternehmen zu verorten ist, sondern auch von außen „eingekauft“ wird. Insofern sollten Unternehmen beim Thema Cybersicherheit immer über die eigenen Unternehmensgrenzen hinweg denken. Gleiches zeigt sich am Beispiel SolarWinds, ein Anbieter von Monitoring-Software für Netzwerke, Systeme und Anwendungen. Hier wurde im Dezember 2020 bekannt, dass Angreifer eine „Hintertür“ in deren Software eingefügt hatten, wodurch sie dann Zugriff auf die Systeme der Unternehmen hatten, die die Software von SolarWinds einsetzten.

Diese Beispiele sind nur ein kleiner Ausschnitt des Gesamtbildes für das gestiegene Risiko von Cyberangriffen. Unternehmen müssen dafür mit einer passenden Cybersecurity gerüstet sein. Ihre aktuellen Einschätzungen dazu zeigen zwei Umfragen, deren Ergebnisse nun dargestellt und eingeordnet werden.

Datengrundlage

Grundlage für die Analyse in diesem Report sind zwei Umfragen. Eine Umfrage wurde zusammen mit dem Marktforschungsinstitut YouGov im Zeitraum vom 11. bis 17. November 2021 durchgeführt. Dabei wurden 254 Personen aus dem IT-Bereich von Unternehmen rund um die Themen Cyberangriffe und Cybersecurity (z. B. Bedrohungslage, Risikofaktoren, Herausforderungen) befragt. Etwa die Hälfte davon sind Unternehmensentscheider mit Führungsverantwortung. Werden im Folgenden Ergebnisse dieser Umfrage vorgestellt, wird der Begriff „IT-Beschäftigte“ verwendet.

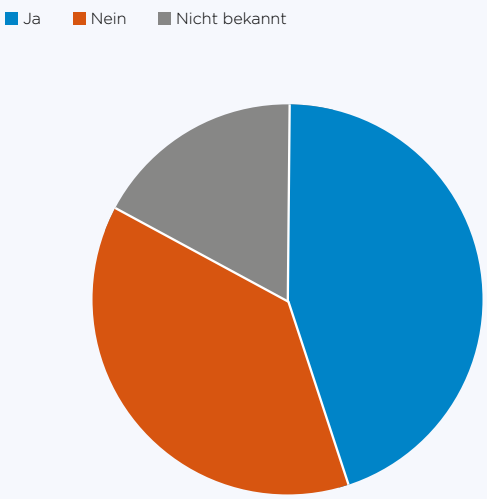
Ergänzend dazu wurde eine zweite Umfrage am 22. November im Rahmen der 11. Handelsblatt Jahrestagung Cybersecurity 2021 durchgeführt. Dazu wurde eine Auswahl der Fragen aus der ersten Umfrage sowie zwei zusätzliche Fragen an die rund 200 Teilnehmenden, bei denen es sich in erster Linie um Chief Information Security Officer (CISO), Cybersecurity-Beschäftigte und hochkarätige IT-Entscheider aus Unternehmen handelt, gestellt. Bei der Live-Umfrage haben im Durchschnitt fast ein Viertel der Teilnehmenden eine Antwort gegeben. Ergebnisse dieser zweiten Umfrage werden über den Begriff „CS-Beschäftigte“ adressiert.

Bedrohungslage und Stand der Cybersicherheit in den Unternehmen

Einleitend wurde bereits das gestiegene Risiko für Cyberangriffe in der jüngsten Zeit hervorgehoben. Dieses kommt auch in den Erfahrungen der Unternehmen zum Ausdruck. Fast die Hälfte der CS-Beschäftigten gibt an, dass sie in ihren Unternehmen in den vergangenen 24 Monaten auf einen Cyberangriff reagieren mussten (siehe Abbildung 1). Nur zwei Fünftel können dies ausschließen. Aber auch bei diesen Unternehmen sowie den Unternehmen, die keine Angaben machten, ist ein Angriff nicht auszuschließend. Denn handelt es sich beispielsweise um einen Advanced Persistent Threat (APT), so zielen die Angreifer genau darauf ab, möglichst unentdeckt zu bleiben.

Abb. 1: Musste das Unternehmen in den vergangenen 24 Monaten auf einen Cyberangriff reagieren?

Anteil der 42 befragten CS-Beschäftigten, in %



Obwohl viele Unternehmen zuletzt auf Angriffe reagieren mussten und zudem die angespanntere Bedrohungslage verstärkt öffentlich diskutiert wird, zeigt sich bei den IT-Beschäftigten kein eindeutiges Bild bei der Einschätzung ihrer künftigen Bedrohungslage. Die Anteile der Befragten, die in den nächsten zwölf Monaten einen Cyberangriff auf ihr Unternehmen als wahrscheinlich bzw. unwahrscheinlich einschätzen, sind nahezu gleich groß (siehe Abbildung 2). Allerdings schätzen die IT-Beschäftigten in größeren Unternehmen das Risiko höher ein.

Selbst wenn nicht alle IT- und CS-Beschäftigen in der Umfrage von einer großen Bedrohung durch Cyberangriffe ausgehen, sollte sich grundsätzlich jedes Unternehmen auf ein höheres Cyberrisiko einstellen. Dazu gehören die passenden Cybersecurity-Maßnahmen. Deren Status quo wird dabei von den befragten Beschäftigten aktuell durchaus positiv eingeschätzt. So sind 70 Prozent der CS-Beschäftigten und vier Fünftel der IT-Beschäftigten der Meinung, dass ihre Unternehmen auf einen Cyberangriff (eher) gut vorbereitet sind (siehe Abbildung 3). Die Unternehmensgröße spielt bei dieser Einschätzung nur bedingt eine Rolle. Einzig die Beschäftigten in Kleinstunternehmen mit bis zu zehn Beschäftigten sind etwas pessimistischer bezüglich der Vorbereitung, wobei auch dort immer noch mindestens die Hälfte diese als (eher) gut beurteilt.

Abb. 2: Wahrscheinlichkeit eines gezielten Cyberangriffs auf das Unternehmen in den kommenden zwölf Monaten

Anteil der befragten IT-Beschäftigten, in %

Differenz zu 100 %: weiß nicht / keine Angabe

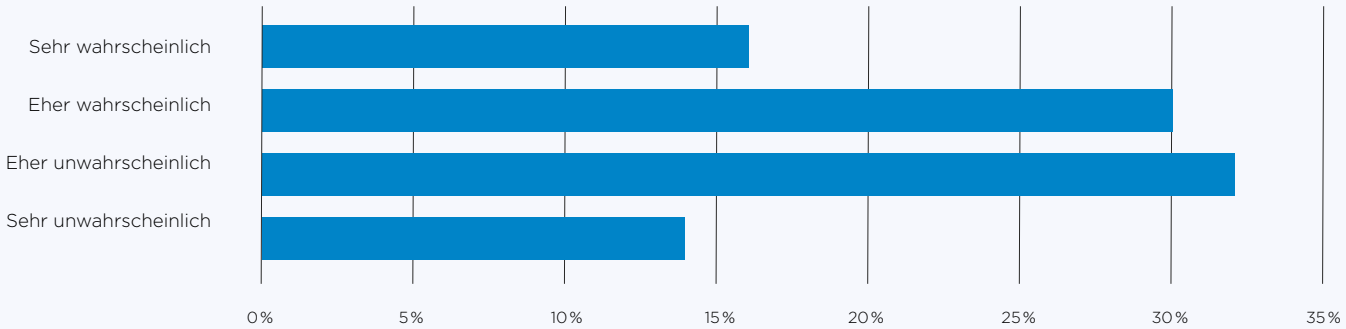


Abb. 3: Wie gut ist das Unternehmen auf einen gezielten Cyberangriff in den kommenden zwölf Monaten vorbereitet?

Anteil der 43 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %

Differenz zu 100 %: weiß nicht / keine Angabe

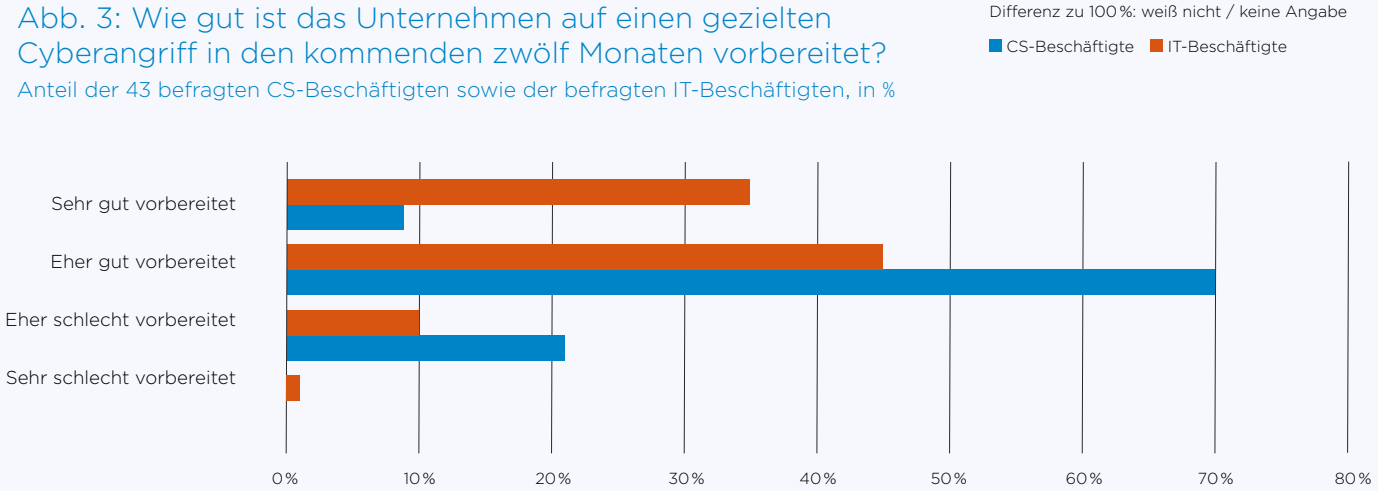
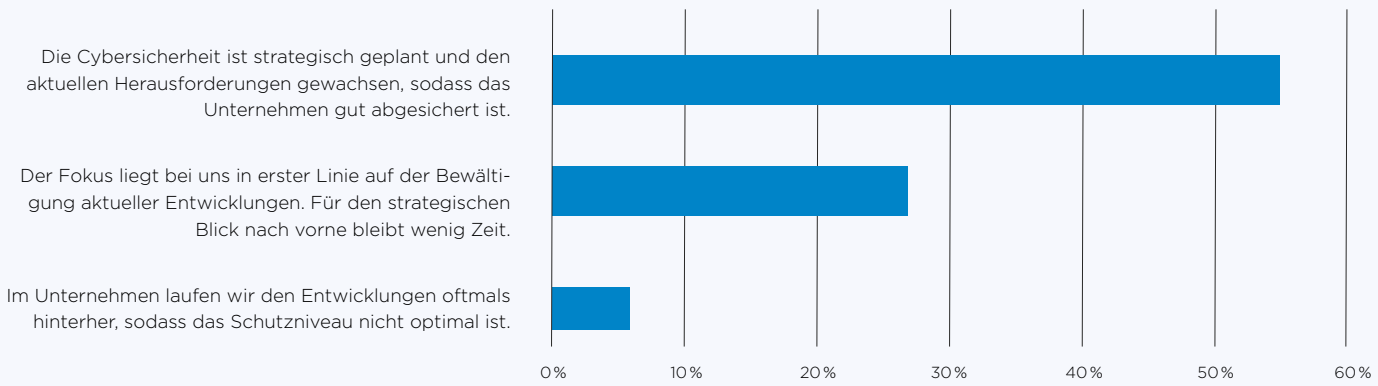


Abb. 4: Stand der Cybersicherheit im Unternehmen

Anteil der befragten IT-Beschäftigten, in %

Differenz zu 100 %: weiß nicht / keine Angabe



Diese positiven Einschätzungen, inwieweit die Unternehmen für einen Angriff gerüstet sind, passen auch zur Beurteilung der Cybersecurity in den Unternehmen der befragten IT-Beschäftigten. Nur sechs Prozent sind der Meinung, dass ihr Unternehmen beim Thema Cybersecurity den Entwicklungen hinterherläuft und insofern kein optimales Schutzniveau aufweist (siehe Abbildung 4). Mehr als vier Fünftel der Befragten sehen ihr Unternehmen hingegen für die Bewältigung der aktuellen Entwicklungen gut gerüstet. Bei einem Teil dieser Unternehmen wird die Cybersecurity allerdings in erster Linie operativ umgesetzt. Zeitbedingt wird eher nur auf aktuelle Entwicklungen reagiert. Etwas mehr als die Hälfte der IT-Beschäftigten sieht in ihren Unternehmen hingegen einen strategischen Umgang bei Planung und Umsetzung der Cybersecurity als gegeben.

Die Cybersecurity ist demnach noch nicht bei allen Unternehmen auf einem adäquaten Niveau, dennoch geht die Entwicklung in die richtige Richtung. Denn ein Großteil der CS-Beschäftigten und mehr als die Hälfte der IT-Befragten sehen für ihr Unternehmen eine Verbesserung des Cybersecurity-Niveaus in den vergangenen zwölf Monaten gegeben (siehe Abbildung 5). Bei den restlichen Unternehmen ist das Niveau zumindest gleichgeblieben, es hat sich so gut wie nie verschlechtert.

Im Vergleich des Cybersecurity-Niveaus mit dem Ausland sind die Befragten eher skeptisch. So überwiegt bei den IT-Beschäftigten marginal die Sichtweise, dass Deutschlands Unternehmen im internationalen Vergleich bei der Abwehr von Cyber-Bedrohungen eher nicht gut dastehen (siehe Abbildung 6). Es gibt insofern noch Verbesserungspotenzial, sodass der bei vielen Unternehmen vorhandene Ausbau der Cybersecurity in den vergangenen zwölf Monaten auch künftig weitergehen muss.

Abb. 5: Wie hat sich das Niveau der Cybersicherheit im Unternehmen über die vergangenen zwölf Monate entwickelt?

Anteil der 43 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %

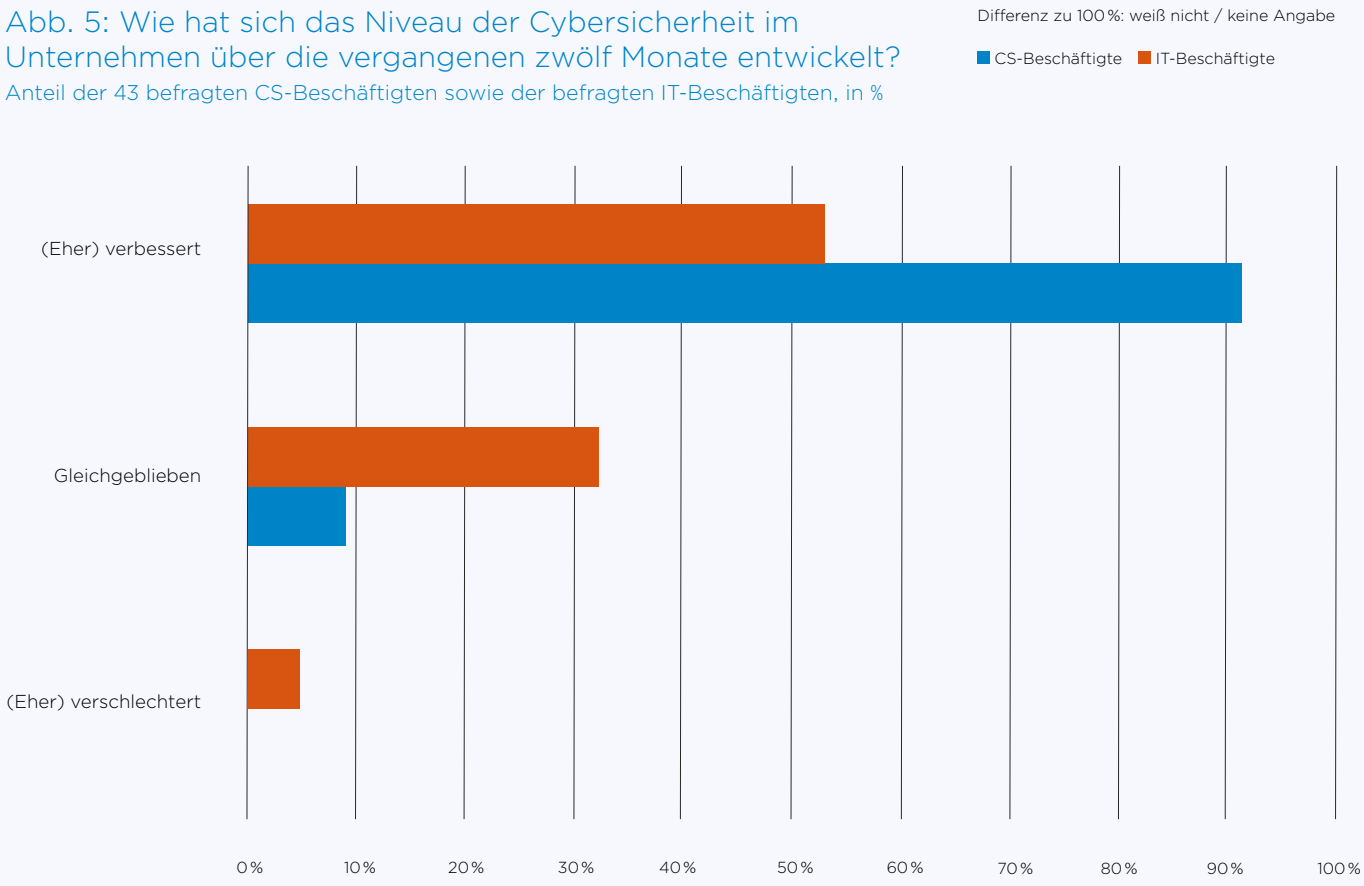
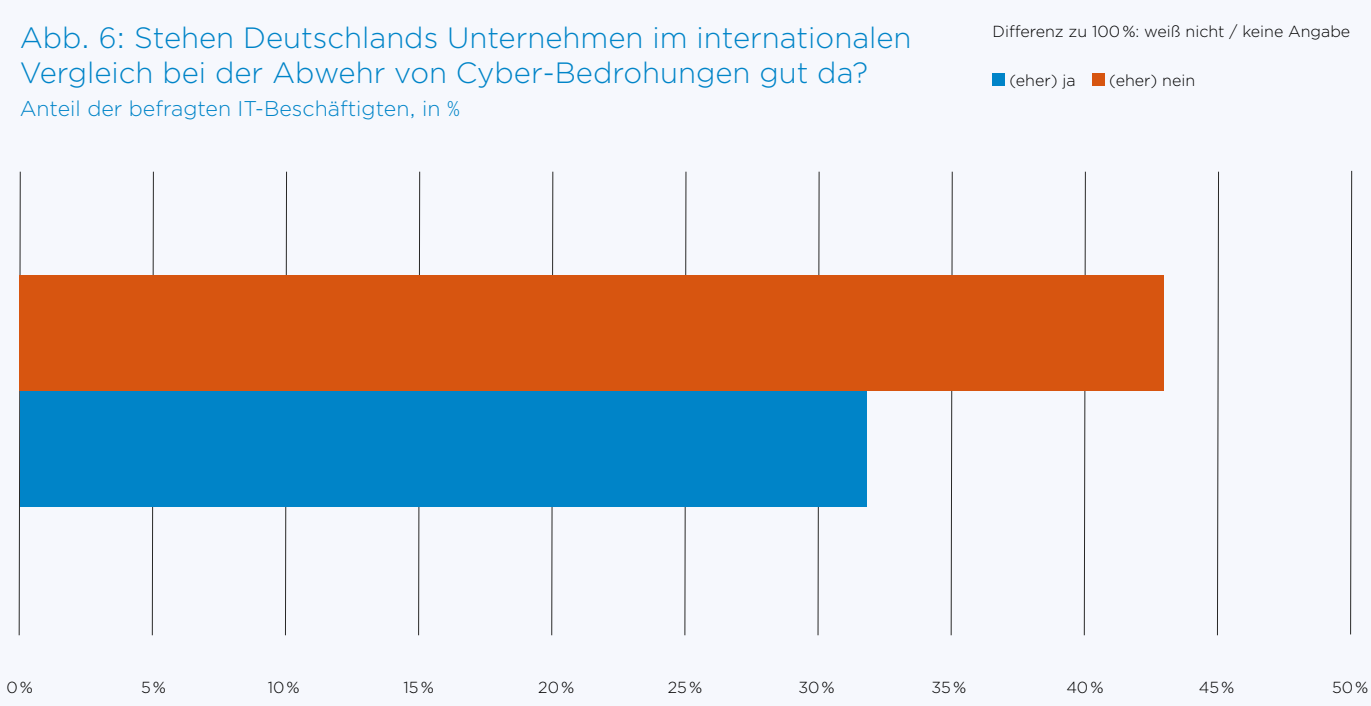


Abb. 6: Stehen Deutschlands Unternehmen im internationalen Vergleich bei der Abwehr von Cyber-Bedrohungen gut da?

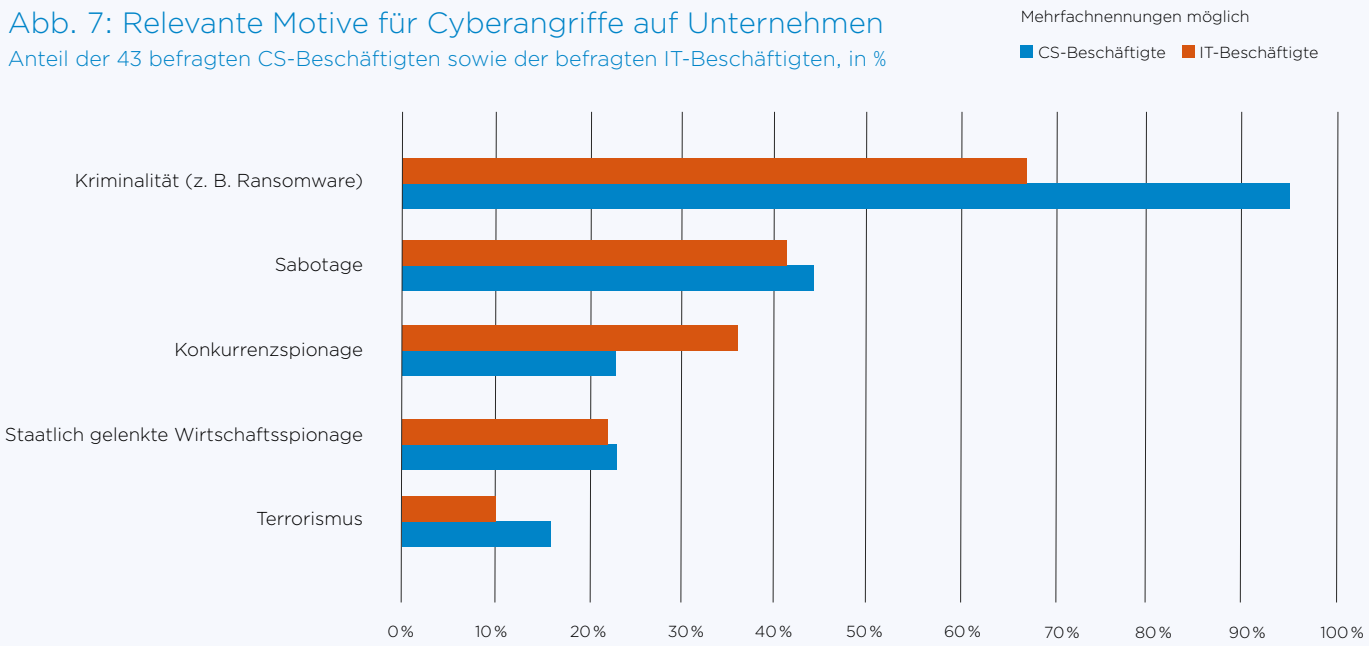
Anteil der befragten IT-Beschäftigten, in %



Cyberangriff – Motive und Angriffsvektoren

Abb. 7: Relevante Motive für Cyberangriffe auf Unternehmen

Anteil der 43 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %



Für Cyberangriffe kommen verschiedene Motive in Betracht. Nach Einschätzung der CS-Beschäftigten sowie der IT-Beschäftigten ist Kriminalität – mit Abstand – das Hauptmotiv für Cyberangriffe (siehe Abbildung 7). Angreifer nutzen beispielsweise Ransomware, um Lösegeld zu erpressen. Zweitwichtigstes Motiv ist Sabotage. Konkurrenzspionage und staatliche Wirtschaftsspionage folgen, wobei die IT-Befragten der Konkurrenzspionage eine vergleichsweise große Bedeutung beimessen. Terrorismus spielt hingegen nach Meinung der CS-Beschäftigten sowie der IT-Beschäftigten als Motiv eine vernachlässigbare Rolle.

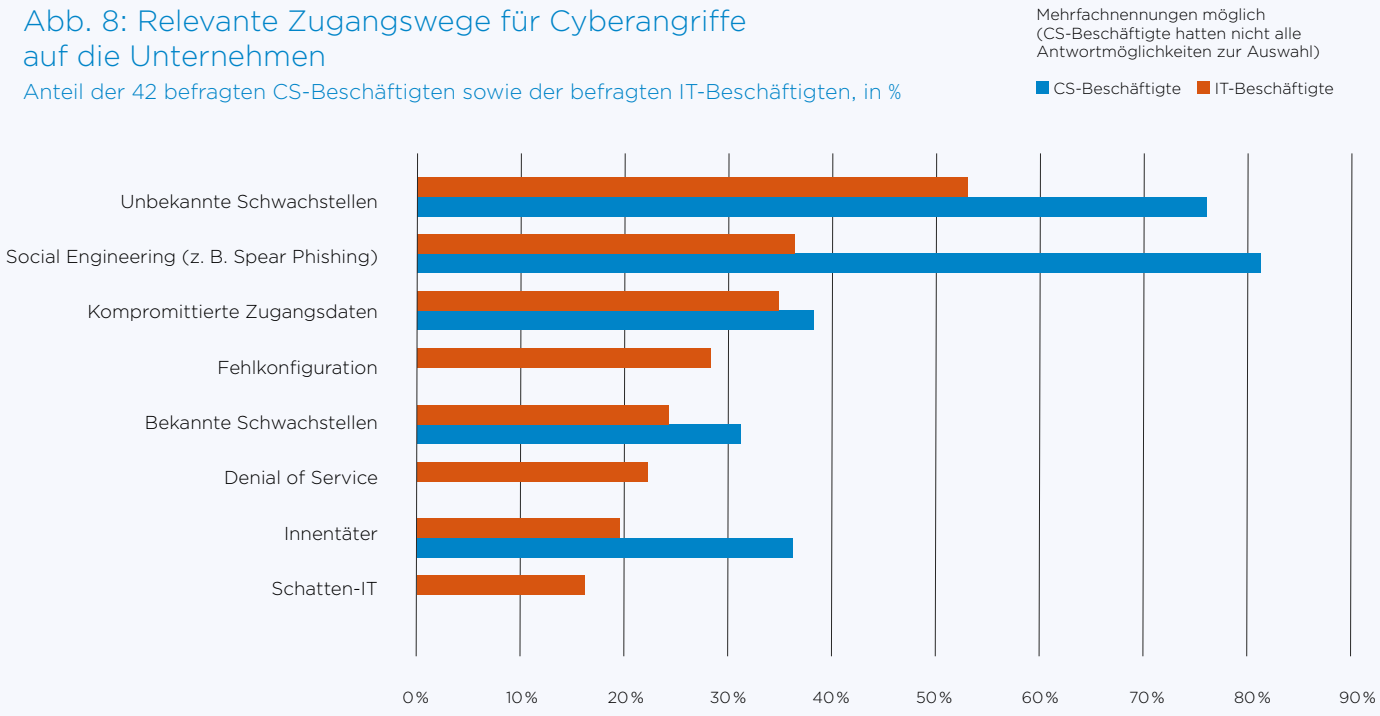
Egal, ob Kriminalität oder Sabotage – der Weg für die Angreifer ins Unternehmen verläuft am Ende meist über den Menschen als wesentlichen „Kanal“. So gehören zu den drei häufigsten Zugangswegen für Cyberangriffe nach Ansicht der Befragten Social Engineering sowie kompromittierte Zugangsdaten (siehe Abbildung 8). Die Angreifer setzen oftmals beim „schwächsten Glied“ in der Sicherheitskette an, welches – ganz ohne Technologie – die Beschäftigten sind. Ihre Daten werden abgeschöpft, worüber dann der Zugang zu den Unternehmenssystemen gelingt.

Oder aber sie werden Opfer eines sogenannten CEO Fraud – ein Betrugskonzept, bei dem Beschäftigte augenscheinlich Anweisungen wie die Durchführung einer Überweisung von der Geschäftsführerin oder dem Geschäftsführer bekommen, allerdings Kriminelle unter Verwendung falscher Identitäten die eigentlichen Absender sind. Mit Fortschritten bei der künstlichen Intelligenz können mittlerweile dabei auch die Stimmen in Telefonanrufen täuschend echt simuliert werden (sogenannte Deepfakes).

Der Großteil der Cyberangriffe erfolgt also nach Meinung der Befragten nicht unmittelbar über die technologische Schiene. Allerdings gehören unbekannte (technologische) Schwachstellen zu den drei wichtigsten Zugangswegen, also Risiken, die die Unternehmen bisher noch nicht im Blickfeld haben. Für die meisten der befragten IT-Beschäftigten sind unbekannte Schwachstellen sogar der häufigste Zugangsweg für die Angreifer. Diese Schwachstellen können dann von Angreifern für sogenannte Zero-Day-Exploits genutzt werden.

Abb. 8: Relevante Zugangswege für Cyberangriffe auf die Unternehmen

Anteil der 42 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %



Unternehmen verfügen demnach über zwei wesentliche Hebel, um sich gegen Cyberangriffe zu wappnen: Erstens müssen die Beschäftigten für das Thema sensibilisiert werden, sodass sie beispielsweise Social-Engineering-Versuche schnell erkennen. Darüber hinaus gilt es für die Unternehmen grundsätzlich, das Sicherheitsniveau hochzuhalten und überall Vorsicht an den Tag zu legen, da ein Angriff über bislang unbekannte Schwachstellen erfolgen kann. Die Cybersecurity wird insofern auch von einem stetigen Screening nach möglichen Schwachstellen ausgemacht.

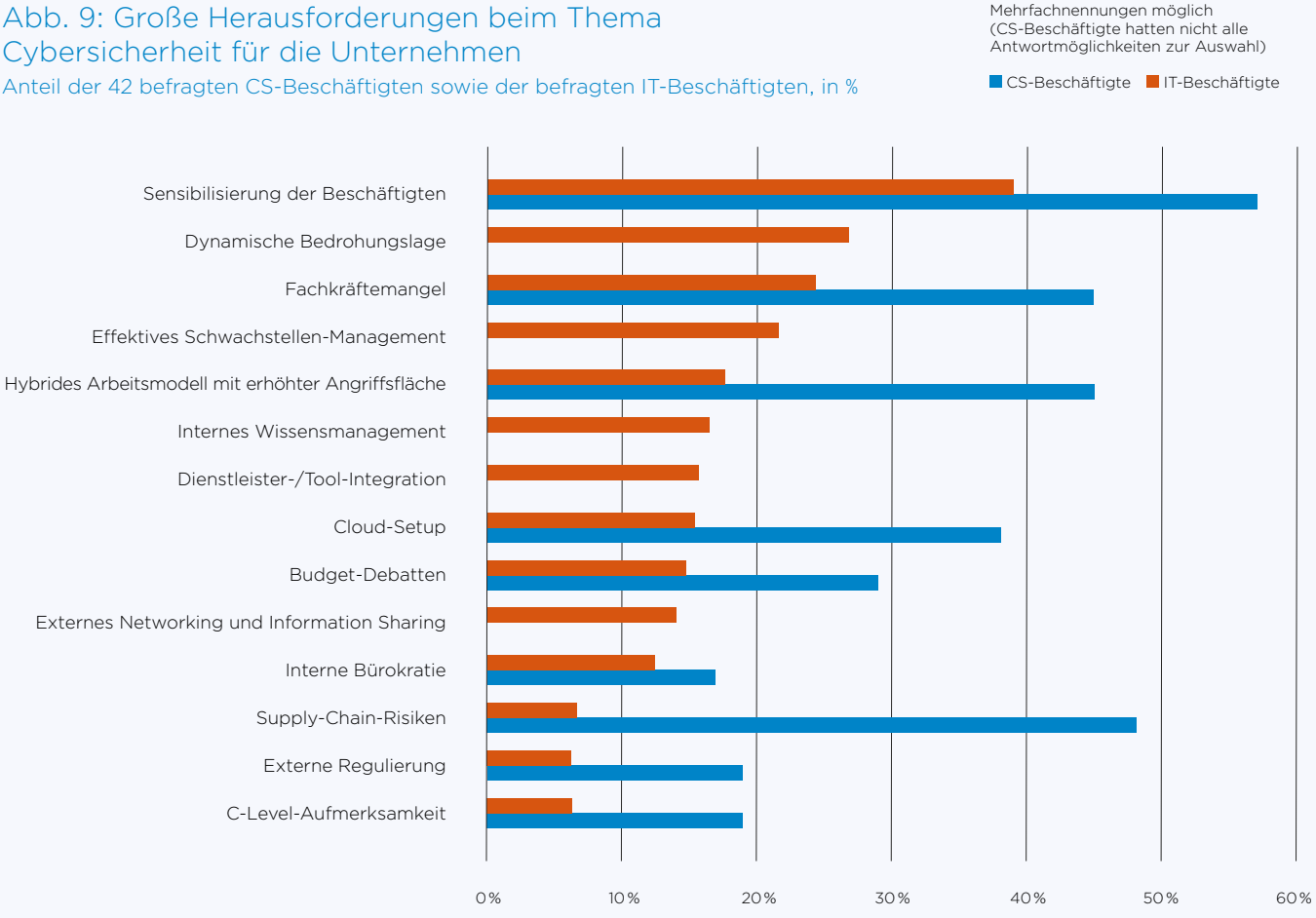
Cybersicherheit – Herausforderungen für die Unternehmen

Angesichts der großen Bedeutung des „menschlichen Faktors“ bei Cyberangriffen, sind die Beschäftigten ebenfalls eine Schlüsselgröße beim Schutz vor solchen Angriffen. Dieses spiegelt sich auch in den Aussagen der befragten CS-Beschäftigten und IT-Beschäftigten zu den größten Herausforderungen für die Unternehmen beim Thema Cybersecurity wider (siehe Abbildung 9). Jeweils für die Mehrheit – 57 Prozent bei den CS-Beschäftigten und 39 Prozent bei den IT-Beschäftigten – ist die Sensibilisierung der Beschäftigten eine zentrale Herausforderung. Diese Einschätzung verdeutlicht abermals, dass Cybersicherheit kein reines Technologiethema ist. Der menschliche Faktor spielt darüber hinaus noch bei einer weiteren großen Herausforderung eine Rolle: dem Fachkräftemangel. Nach Einschätzung der Befragten, ist die Suche nach passenden Cybersecurity-Fachkräften für ihre Unternehmen durchaus sehr herausfordernd.

Abb. 9: Große Herausforderungen beim Thema Cybersicherheit für die Unternehmen

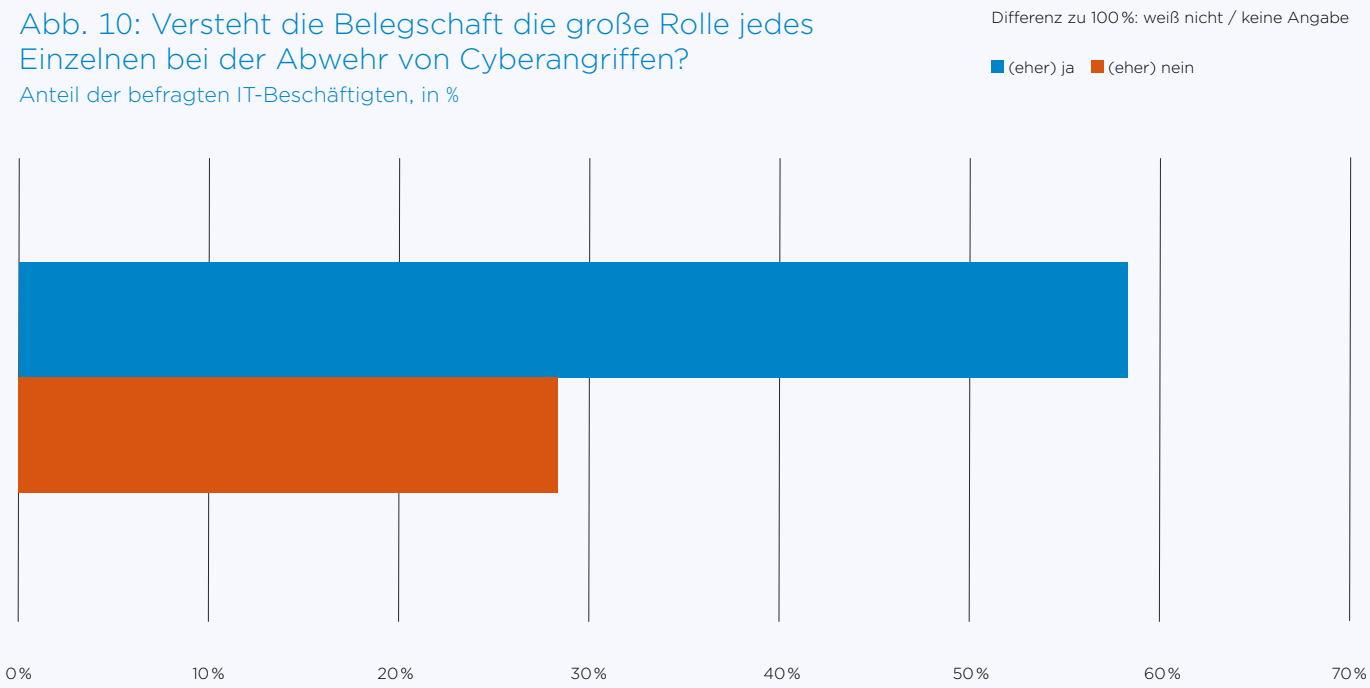
Anteil der 42 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %

Mehrfachnennungen möglich
(CS-Beschäftigte hatten nicht alle Antwortmöglichkeiten zur Auswahl)



Förderlich für die weitere Sensibilisierung der Mitarbeiter ist, dass nach Einschätzung von ungefähr drei Fünftel der befragten IT-Beschäftigten die Belegschaft in deren Unternehmen die wichtige Rolle jedes Einzelnen bei der Abwehr von Cyberangriffen versteht (siehe Abbildung 10). Darauf sollten sich die Unternehmen allerdings nicht ausruhen. Alle Beschäftigten müssen sensibilisiert sein und ihre Bedeutung bei der Abwehr von Cyberangriffen kennen.

Abb. 10: Versteht die Belegschaft die große Rolle jedes Einzelnen bei der Abwehr von Cyberangriffen?
Anteil der befragten IT-Beschäftigten, in %



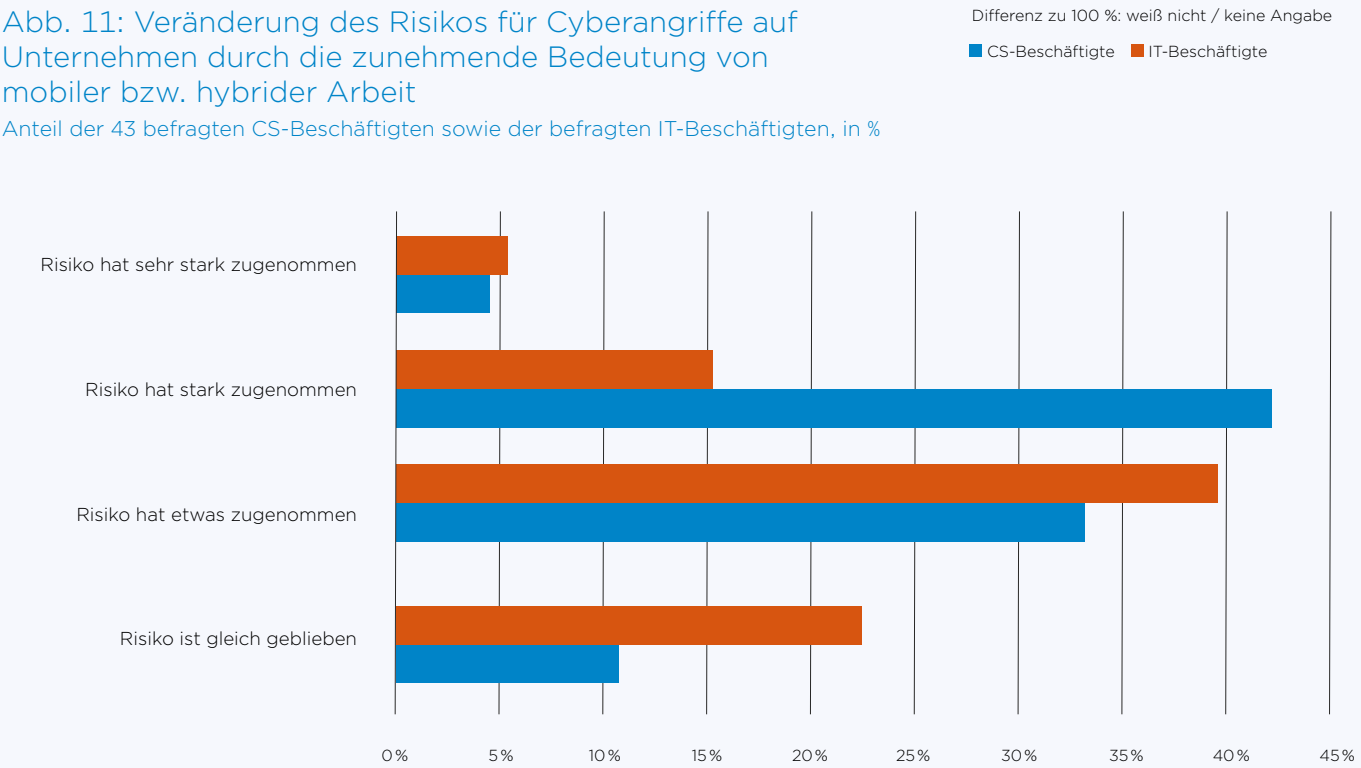
Darüber hinaus gehören für die IT-Beschäftigten zu den vier größten Herausforderungen zudem die dynamische Bedrohungslage sowie ein effektives Schwachstellen-Management (siehe Abbildung 9). Gerade Letzteres ist bei der hohen Relevanz unbekannter Schwachstellen als Angriffsvektor sehr wichtig (siehe Abbildung 8).

Die CS-Beschäftigten heben neben der Sensibilisierung der Beschäftigten sowie dem Fachkräftemangel noch die Supply Chain Risiken sowie das hybride Arbeitsmodell als große Herausforderung hervor (siehe Abbildung 9). Cybersicherheit darf demnach nicht nur innerhalb der Grenzen des eigenen Unternehmens gedacht werden, sondern umfasst auch Schwachstellen bei Unternehmen, mit denen man entlang der Wertschöpfungskette „verbunden“ ist, da sie das eigene Unternehmen bedrohen. Dies verdeutlichte der Fall SolarWinds.

Eine weitere Herausforderung beim Thema Cybersecurity ist eine Folge der Coronapandemie. Zur Eindämmung der Infektionsausbreitung haben viele Unternehmen – zum Teil staatliche verordnet – innerhalb kurzer Zeit mobiles Arbeiten eingeführt. Auch nach dem Ende der Pandemie werden die Beschäftigten vermehrt mobiles Arbeiten beziehungsweise eine Mischung aus Arbeit im Büro und mobilem Arbeiten – hybrides Arbeiten – präferieren. Damit ist in Bezug auf die Cybersicherheit ein zusätzliches Risikopotenzial verbunden – so jedenfalls ist die Einschätzung der CS-Beschäftigten und IT-Beschäftigten. Nur eine Minderheit der Befragten sagt aus, dass das Risiko für Cyberangriffe auch bei vermehrter Nutzung von mobilem und hybriden Arbeiten gleich bleibt (siehe Abbildung 11). Der Großteil ist davon überzeugt, dass mit dieser Arbeitsform das Risiko zunimmt. Ursächlich hierfür könnten begünstigende Aspekte wie Remotezugriffe auf das Unternehmensnetzwerk sowie verstärkte Nutzung von privaten Geräten sein.

Abb. 11: Veränderung des Risikos für Cyberangriffe auf Unternehmen durch die zunehmende Bedeutung von mobiler bzw. hybrider Arbeit

Anteil der 43 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %



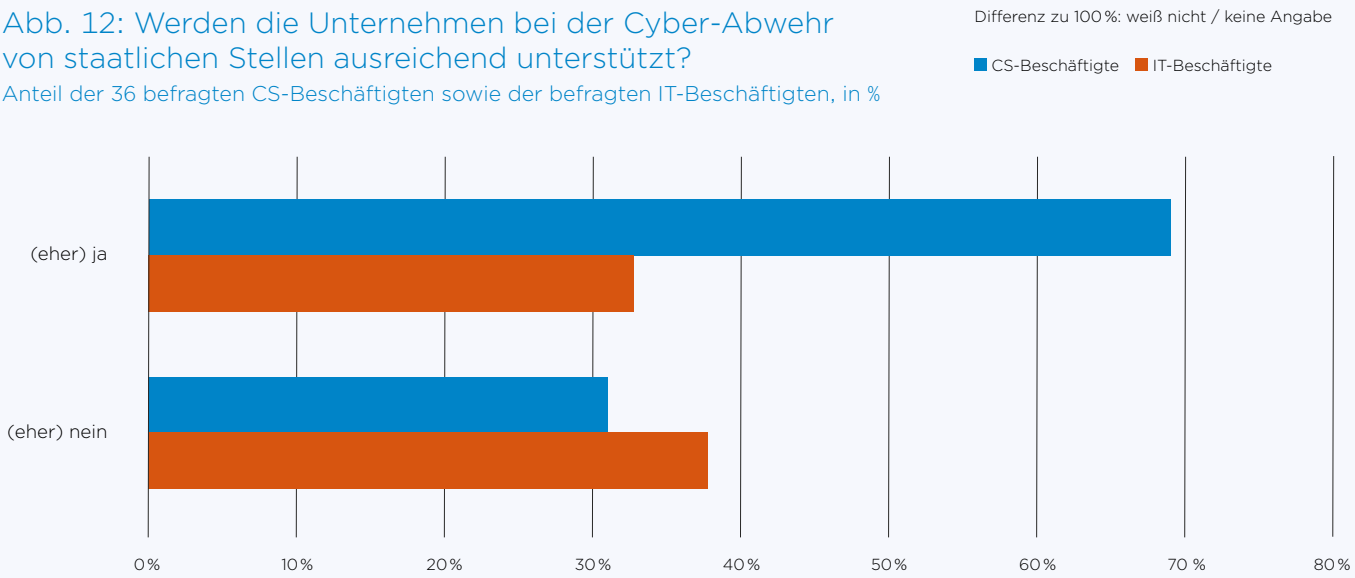
Rahmenbedingungen

Die Abwehr von Cyberangriffen sowie ein möglichst hohes Cybersecurity-Niveau liegen in erster Linie im Verantwortungsbereich der Unternehmen. Allerdings erhalten sie auch Unterstützung von staatlicher Seite, da Cybersicherheit ebenfalls zum Bereich der öffentlichen Sicherheit gehört und insofern in Teilen auch eine staatliche Aufgabe ist.

Beim Ausmaß dieser Unterstützung unterscheiden sich allerdings die Einschätzungen der befragten CS-Beschäftigten und der IT-Beschäftigten. So betrachten etwas mehr als zwei Drittel der CS-Beschäftigten die staatliche Unterstützung ihrer Unternehmen bei der Abwehr von Cyberangriffen als ausreichend (siehe Abbildung 12). Hingegen schätzen die befragten IT-Beschäftigten dies nicht ganz so positiv ein. Bei ihnen überwiegt marginal die Meinung, dass sich ihr Unternehmen bei der Abwehr von staatlicher Seite eher nicht ausreichend unterstützt wird.

Abb. 12: Werden die Unternehmen bei der Cyber-Abwehr von staatlichen Stellen ausreichend unterstützt?

Anteil der 36 befragten CS-Beschäftigten sowie der befragten IT-Beschäftigten, in %



Positiver ist die Einschätzung der IT-Beschäftigten hingegen in Bezug auf das Innovationsniveau im privaten Cybersecurity-Markt. Mit etwa zwei Fünftel der Befragten teilt die (relative) Mehrheit die Meinung, dass die Innovationen dort ausreichen, um den aktuellen Herausforderungen zu begegnen (siehe Abbildung 13).

Beim Umgang mit Cyberangriffen haben in der Vergangenheit die Unternehmen Hilfe von der Polizei und dem Bundesamt für Sicherheit in der Informationstechnik in Anspruch genommen. Der Staat bietet den Unternehmen auch Unterstützung bei der Prävention an. Bei diesem Thema können sich die Unternehmen auch gegenseitig helfen und die Cybersicherheit gemeinsam verbessern. Hierfür sind unter anderem eine gute Vernetzung sowie ein reger Informationsaustausch innerhalb der Community wichtig. Und genau dies ist nach Ansicht von mehr als zwei Fünftel der befragten IT-Beschäftigten auch gegeben (siehe Abbildung 14).

Dabei gibt es immer noch Verbesserungspotenzial. So kann nach Ansicht der befragten CS-Beschäftigten die Zusammenarbeit aller Beteiligten – Bund, Länder, Unternehmen – bei der Cybersicherheit am ehesten durch diese beiden Aspekte – einen intensiveren Informationsaustausch sowie eine bessere Koordination der verschiedenen Initiativen – verbessert werden. Insofern kommt es weniger auf mehr gesetzliche Regelungen oder Forschungsförderung an, die nur für einige wenige Befragte die Zusammenarbeit verbessern würde.

Abb. 13: Reichen die Innovationen im privaten Cyber-Security-Markt für die aktuellen Herausforderungen aus?

Anteil der befragten IT-Beschäftigten, in %

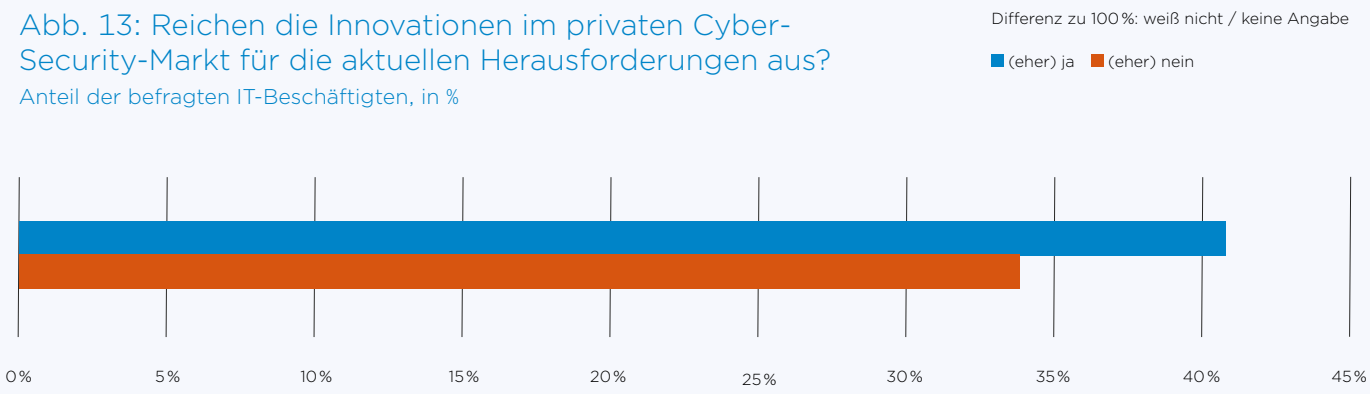


Abb. 14: Ist die deutsche IT-Sicherheitscommunity gut vernetzt und findet ein reger Informationsaustausch statt?

Anteil der befragten IT-Beschäftigten, in %

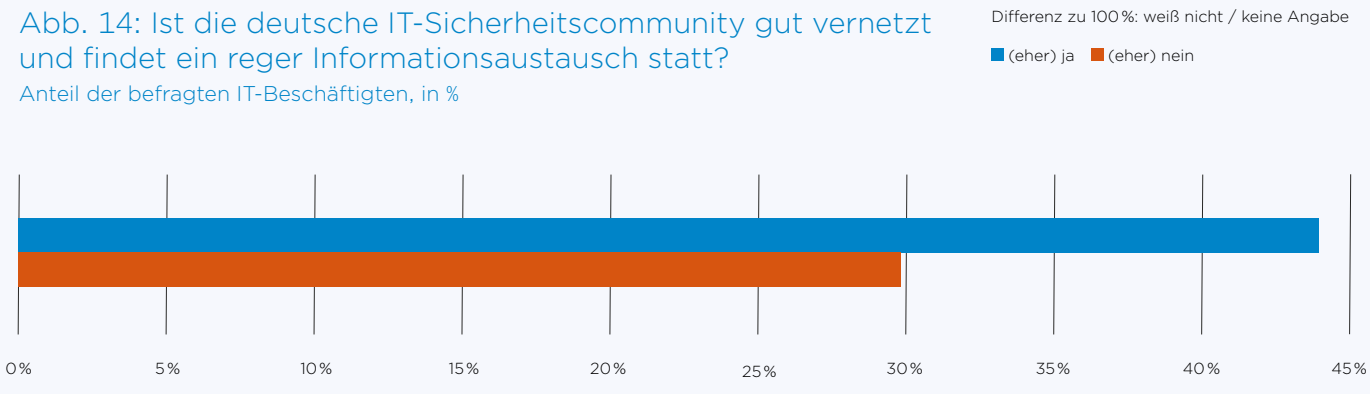
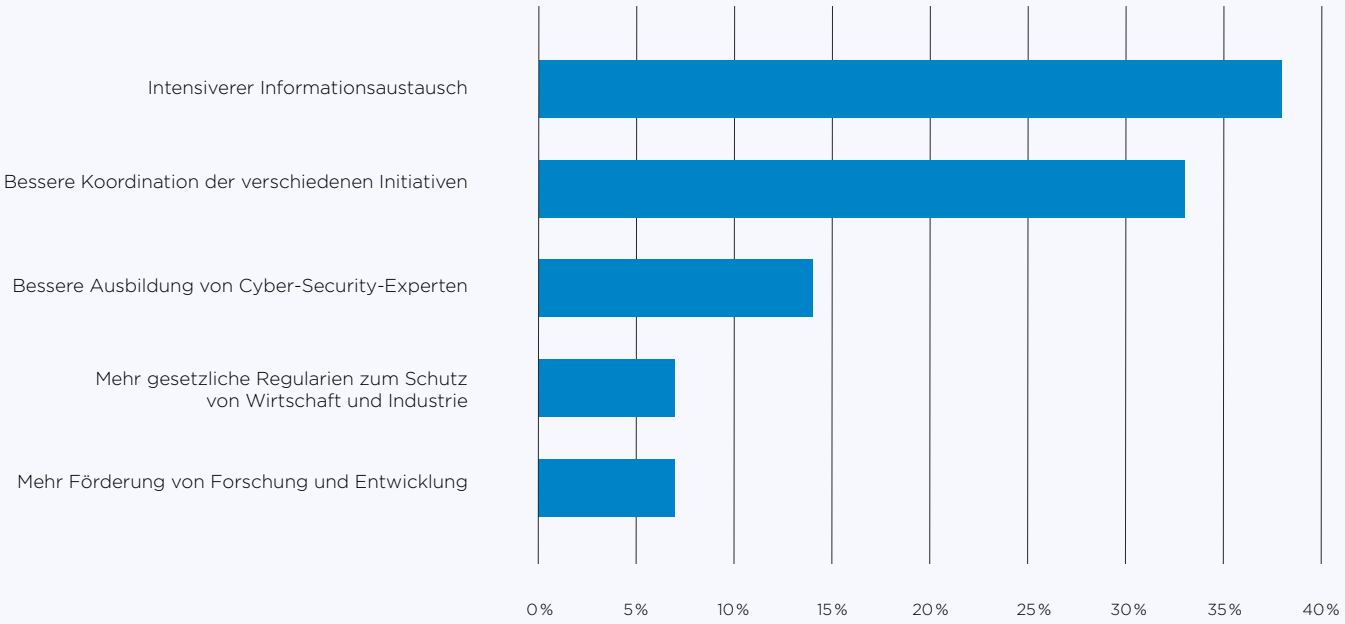


Abb. 15: Verbesserungsvorschläge für die Zusammenarbeit von Bund, Ländern und Unternehmen im Bereich Cyber-Sicherheit

Anteil der 42 befragten CS-Beschäftigten, in %



Interview

mit Frank Ziarno, Vice President Product Management, TeamViewer

Die Befragten sehen ihre Unternehmen im Großen und Ganzen gut auf künftige Cyberangriffe vorbereitet. Wie ist hier Ihre Einschätzung? Sind die Unternehmen in Deutschland in Sachen Cybersicherheit gut aufgestellt?

Eine grundsätzliche Aussage hierzu zu treffen, ist natürlich nicht leicht. Es ist davon auszugehen, dass insbesondere größere Unternehmen über Personal verfügen, welches sich dediziert dem Thema Cybersicherheit widmet und damit eine gewisse Weitsicht in die jeweilige Sicherheitsstrategie bringt. Denn es gilt: Zwischen den Cybersicherheits-Experten und den Cyber-Kriminellen herrscht ein permanentes Wettrüsten. Unternehmen, ungeachtet ihrer Größe, müssen sich unbedingt die Frage stellen, ob ihre Sicherheitsstrategie auch eine Reaktion auf zukünftige, jetzt noch unbekannte Bedrohungen zulässt. Zudem hat nicht zuletzt die Pandemielage und die damit verbundene Verlagerung ins Homeoffice neue Herausforderungen hinsichtlich der Cybersicherheit geschaffen. Es lohnt sich also nochmal genauer hinzuschauen.

Unbekannte Schwachstellen spielen nach Ansicht der Befragten als Zugangsweg für Cyberangriffe auf Unternehmen eine große Rolle. Gibt es Möglichkeiten, wie Unternehmen hier Angriffsrisiken verringern können?

Angriffe über unbekannte Schwachstellen, oder auch Zero-Day-Exploits, wurden von traditionellen (oft rein signaturbasierten) Sicherheitslösungen oft nicht erkannt. Moderne Sicherheitslösungen setzen zu großen Teilen auf signaturlosen Schutz mithilfe von künstlicher Intelligenz und maschinellem Lernen. Dadurch wird ein höherer Schutzgrad erzeugt, welcher Bedrohungslagen zuverlässig antizipiert und somit auch einen Schutz gegen unbekannte Schwachstellen bietet. Unternehmen sollten also unbedingt einen Paradigmenwechsel hin zu einer Zero-Trust-Strategie vollführen, bei welcher eine moderne Sicherheitslösung, oder NGAV (Next-Generation Antivirus), eine zentrale Rolle einnimmt. Auch das regelmäßige patchen aller Systeme verringert die Angriffsrisiken weiter. Auch wenn Zero-Day-Exploits dadurch natürlich nicht verhindert werden, können die Auswirkungen im weiteren Verlauf der Angriffskette potenziell weniger drastisch ausfallen, z. B. wenn durch den Zero-Day-Exploit weitere (bekannte und gepatchte) Schwachstellen ausgenutzt werden sollen.

Welches Potenzial ist mit neuen technologischen Möglichkeiten wie künstlicher Intelligenz beim Thema Cybersicherheit verbunden?

Künstliche Intelligenz und maschinelles Lernen bergen ein großes Potenzial und sind aus der Cybersicherheit nicht mehr wegzudenken. So lernt die künstliche Intelligenz beispielsweise typische Verhaltensmuster innerhalb der IT-Infrastruktur eines Unternehmens und tut dies weitaus effizienter, als es ein Mensch je könnte. Wird diese IT-Infrastruktur durch einen externen Akteur infiltriert, löst das Abweichen vom Verhaltensmuster einen Alarm aus. Die Möglichkeiten enden nicht an dieser Stelle. Wie bereits erwähnt, ist die Cybersicherheit eine Art Wettrüsten und die künstliche Intelligenz hilft bei zunehmender Datenmenge und wachsender Anzahl unterschiedlichster Angriffsmethoden handlungsfähig und geschützt zu bleiben.

Was sind aus Ihrer Sicht wesentliche Fehler, die Unternehmen beim Thema Cybersicherheit machen, oder Aspekte, die unterschätzt werden?

Fehlende Backups, keine komplette Übersicht über die eigene IT-Infrastruktur und ein Vernachlässigen des Patch Managements sind oft gemachte, aber vermeidbare Fehler. Auch der Faktor Mensch sollte nicht unterschätzt werden. Die Anzahl von sogenannten Cyber-Anfängern in Deutschland nimmt stetig ab, doch Fehleinschätzungen sind alles andere als eine Ausnahme. Es lohnt sich also in Trainings zu investieren, die das Bewusstsein der Belegschaft für Cybergefahren schärft.

Abgesehen davon ist es ratsam in regelmäßigen Abständen Penetrationstests von außen durchzuführen und Bedrohungsanalysen zu fahren. Grundsätzlich ist es nicht verkehrt auch die eigene Geschäftsführung hinsichtlich Cybersicherheit zu sensibilisieren, insbesondere mithilfe der Darstellung finanzieller sowie Reputationsschäden im Falle eines erfolgreichen Angriffs, um der Sicherheitsstrategie so mehr Relevanz und Aufmerksamkeit zu verleihen.

Handelsblatt
RESEARCH INSTITUTE

Das **Handelsblatt Research Institute (HRI)** ist ein unabhängiges Forschungsinstitut unter dem Dach der Handelsblatt Media Group. Es schreibt im Auftrag von Kundinnen und Kunden, wie Unternehmen, Finanzinvestoren, Verbänden, Stiftungen und staatlichen Stellen wissenschaftliche Studien. Dabei verbindet es die wissenschaftliche Kompetenz des 30-köpfigen Teams aus Ökonom:innen, Sozial- und Naturwissenschaftler:innen sowie Historiker:innen mit journalistischer Kompetenz in der Aufbereitung der Ergebnisse.
Es arbeitet mit einem Netzwerk von Partner:innen sowie Spezialist:innen zusammen.
Daneben bietet das Handelsblatt Research Institute Desk-Research, Wettbewerbsanalysen und Marktforschung an.

Konzept, Recherche und Gestaltung:
Handelsblatt Research Institute
Toulouser Allee 27
40211 Düsseldorf
www.handelsblatt-research.com

Autoren: Dr. Sven Jung
Layout: Isabel Rösler, Ilka Schlegtendal

Düsseldorf, Januar 2022

Bildquellen: Freepik