www.pwc.de/dti2022

PwC Global Digital Trust Insights Survey 2022

Der C-Suite Leitfaden für Cybersicherheit

pwc

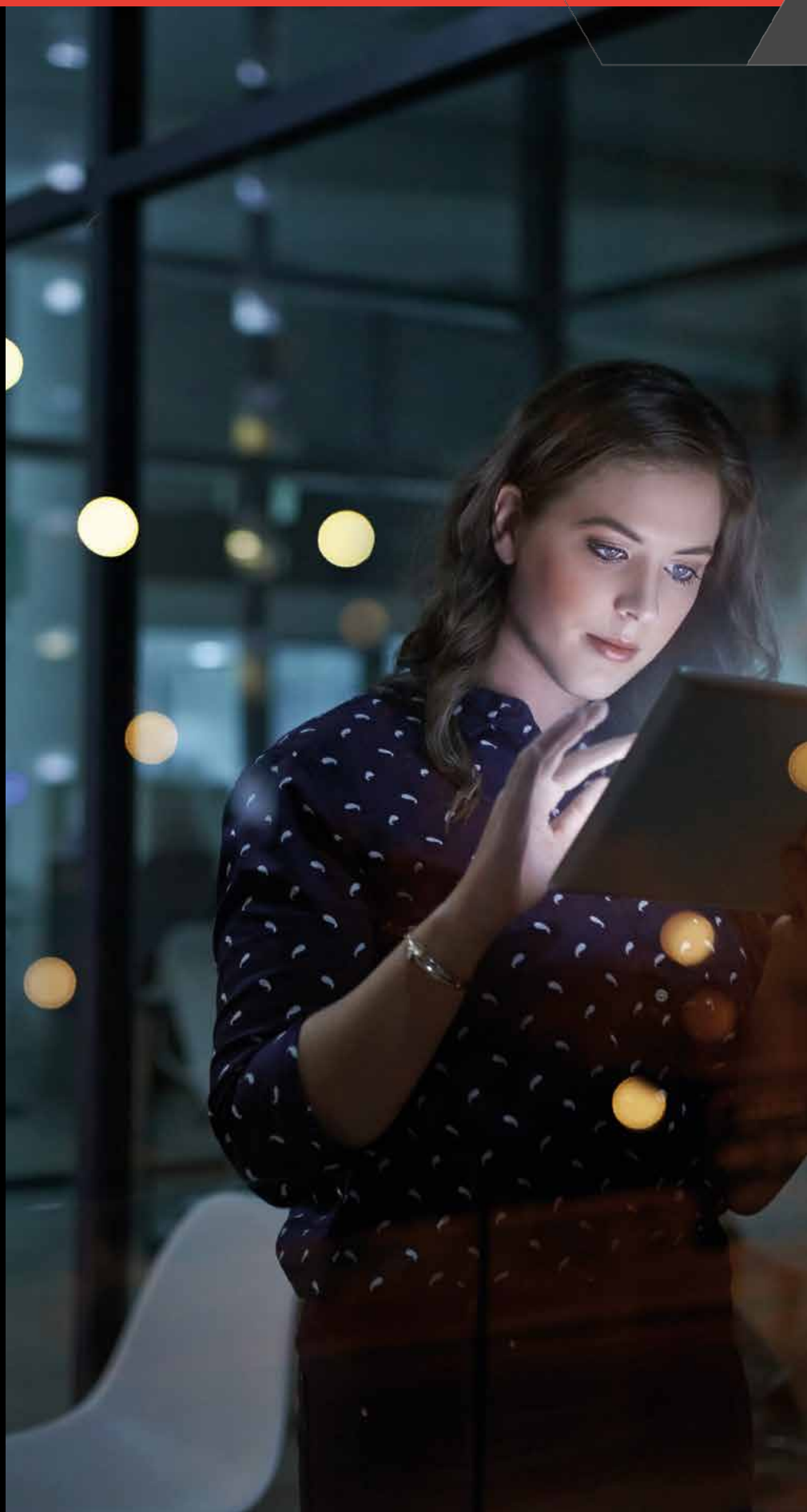
Wie Cybersicherheit heute und morgen einfacher gelingt

In einer übermäßig komplexen Organisation kann es leicht passieren, dass die linke Hand nicht weiß, was die rechte Hand tut – und das kann schlimme Folgen für die Cybersicherheit und den Datenschutz haben. 82 Prozent der befragten Führungskräfte in Deutschland, darunter auch CISOs, geben an, dass ihre Unternehmen zu komplex sind – und zwar in vermeidbarer, überflüssiger Weise – und fast ebenso viele sagen, dass die Komplexität in 11 Schlüsselbereichen besorgniserregende Cyber- und Datenschutzrisiken für ihr Unternehmen darstellt.

Die Folgen eines Angriffs nehmen zu, je komplexer die Abhängigkeiten zwischen unseren Systemen werden. Kritische Infrastrukturen sind besonders verwundbar. Immer raffiniertere Angreifer durchforsten die dunklen Ecken unserer Systeme und Netzwerke, suchen – und finden – Schwachstellen.

Wie auch immer die digitale Achillesferse einer Organisation beschaffen sein mag – Angreifer werden alle ihnen zur Verfügung stehenden Mittel einsetzen, sowohl herkömmliche als auch hochentwickelte, um diese Schwachstellen auszunutzen.

Und doch lassen sich viele der Angriffe, die wir erleben, mit soliden Cyberpraktiken und starken Kontrollen verhindern. Wie Führungskräfte die Herausforderungen und Chancen im Bereich Cyber Security bewerten, haben wir in der diesjährigen Befragung der *„Global Digital Trust Insights“* beleuchtet.

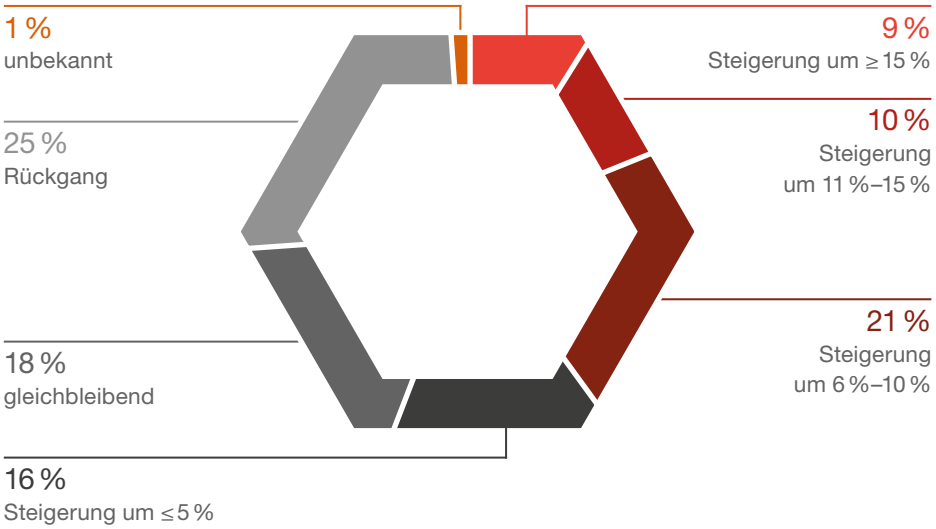


Die Studie im Überblick

Investitionen steigen

Die Investitionen in Cybersicherheit wachsen beständig. 56 Prozent (Global: 69 Prozent) der Unternehmen in Deutschland sagen für 2022 einen Anstieg der Cyberbudgets voraus, verglichen mit 51 Prozent im letzten Jahr. Besonders auffällig: In Deutschland ist der Prozentsatz derjenigen, die mit einem Budget-Anstieg größer 10 Prozent rechnen, von 5 Prozent auf 19 Prozent gestiegen.

Abb. 1 Wie wird sich ihr Cyber-Budget im Jahr 2022 entwickeln?



Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Deutschland.

Simplifying cyber

Mit der sprunghaften Vermehrung digitaler Verbindungen entstehen komplexere Netze, die mit jeder neuen Technologie immer noch komplexer werden. Ein Smartphone ist zugleich Telefon, Kamera, Kalender, Fernseher, Gesundheitsmessgerät, eine ganze Bibliothek von Büchern und vieles mehr. Das vereinfacht unser Leben in vielerlei Hinsicht und ermöglicht es uns, auch unterwegs produktiv zu sein. Das Internet der Dinge lässt uns unzählige Aufgaben mit einem einfachen Befehl ausführen, Fabriken fast wie von selbst steuern und unsere Gesundheit aus der Ferne überwachen.

Aber auch die Prozesse, die zur Verwaltung und Aufrechterhaltung all dieser Verbindungen erforderlich sind – einschließlich der Cybersicherheit – werden immer komplizierter.

Sicherheit in der Unsicherheit

Ist die Geschäftswelt bereits zu komplex, um sie zu sichern? Führungskräfte schlagen Alarm. Etwa 75 Prozent der globalen Befragten der PwC-Studie „Global Digital Trust Insights 2022“ sind besorgt über zu viel vermeidbare, unnötige organisatorische Komplexität und damit verbundene Cyber- und Datenschutzrisiken.

Was ist notwendig, was nicht? Ihr Unternehmen sollte seine Abläufe und Prozesse bewusst und mit Bedacht rationalisieren und vereinfachen.

Abb. 2 Cybersecurity-Scorecards: 4 von 10 Unternehmen berichten in vier Bereichen über deutliche Fortschritte in den letzten zwei Jahren

Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Global.

Leitfaden zur Vereinfachung

Die Global Digital Trust Insights Survey 2022 bietet der Führungsebene einen Leitfaden für die bewusste Vereinfachung von Cyber Security. Sie konzentriert sich auf vier Fragen, die im Unternehmensalltag zu kurz kommen, aber erhebliche Vorteile bringen können.

Überraschend: Diese Fragen sind nicht technologieorientiert. Technik an sich ist nicht unbedingt der Schlüssel zu mehr Cyber Security. Wir konzentrieren uns stattdessen auf die Zusammenarbeit als Team, von der Technik bis zur Vorstandsetage – angefangen beim CEO an der Spitze. Cyber Security ist ein Thema für das gesamte Unternehmen, in jeder Funktion und für jeden Mitarbeitenden.

1. Wie können CEOs die Cybersicherheit in ihren Unternehmen verbessern?
2. Ist Ihr Unternehmen zu komplex, um es zu sichern?
3. Sichern Sie Ihre Organisation gegen die wichtigsten Risiken von heute und morgen ab?
4. Wie gut kennen Sie die Risiken Dritter und der Lieferkette?

Anhand von Antworten auf diese Fragen haben wir die 10 Prozent der Unternehmen ermittelt, die in Cyber Security am fortschrittlichsten sind. Bei diesen Cyber-Pionieren ist die Wahrscheinlichkeit enorm hoch, dass sie deutliche Fortschritte bei wichtigen Cyber-Zielen verzeichnen:

- Einführung einer Kultur der Cybersicherheit,
- Management von Cyberrisiken,
- Verbesserung der Kommunikation zwischen Vorstand und Management
- und Abstimmung der Cyberstrategie mit der Geschäftsstrategie.

Abb. 3 Unternehmen, die modernste Methoden und Techniken einsetzen, haben auch die größten Fortschritte in der Cybersecurity.

Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Global.

Vielfache Wirkung

Digitale Geschäftsmodelle haben das Potenzial, den Erfolg eines Unternehmens um das Zehnfache zu steigern. Die PwC-Studie zeigt, dass in der Vereinfachung von Geschäftsprozessen ein vergleichbar großer Multiplikatoreffekt in Bezug auf Cyber Security und Datenschutz liegen kann.

Die Erfolgsfaktoren, die bei den am weitesten fortgeschrittenen und optimierten Organisationen zu beobachten sind, können als die „4 P“ zur Ausschöpfung des vollen Cyber-Potenzials bezeichnet werden: Principle, People, Priorities, Perception.

Principle. Die CEOs müssen ein klares Grundprinzip formulieren, das Sicherheit und Datenschutz zu einem geschäftlichen Gebot macht.

People. Stellen Sie die richtigen Führungskräfte ein und lassen Sie den CISO und die Sicherheitsteams mit den Fachteams zusammenarbeiten. Ihre Mitarbeitenden können zu Vorreitern in puncto Vereinfachung werden, während Sie im Unternehmen eine „gute Komplexität“ aufbauen.

Priorities. Ihre Risiken ändern sich ständig, wenn Ihre digitalen Aktivposten wachsen. Nutzen Sie Daten und Informationen, um Ihre Risiken kontinuierlich zu messen.

Perception. Was man nicht sieht, kann man nicht sichern. Decken Sie „blinde Flecken“ in Ihren Beziehungen und Lieferketten auf.

So vernünftig diese Grundsätze und Praktiken auch erscheinen mögen, sie sind nicht alltäglich. Nur die besten 10 Prozent der Unternehmen halten sie ein – und auch sie berichten, dass sie in den letzten zwei Jahren erhebliche Fortschritte bei der Erreichung ihrer Cyber-Ziele gemacht haben.

Neue Wege wagen

Auf der anderen Seite kämpfen viele Unternehmen weiterhin mit komplexen Strukturen. Oft sind schlechte Gewohnheiten der Grund dafür:

- Der Einsatz vieler technischer Einzellösungen, die nicht aufeinander abgestimmt sind.
- Fehlende Koordinierung der Arbeit verschiedener Funktionen in Bezug auf Ausfallsicherheit oder Risikomanagement für Dritte.
- Fehlende Prozesse für den Umgang mit Daten (Governance).

Unternehmen entwickeln diese schlechten Gewohnheiten, weil etwas schnell gehen muss, oder sie akzeptieren und übernehmen unfertige Lösungen, weil es Widerstand gegen Veränderungen gibt. Aber schlechte Gewohnheiten kann man abgelegen. Und C-Level-Champions können dabei helfen, neue Gewohnheiten der Koordination und Zusammenarbeit zwischen allen Funktionen, Unternehmen und Technik zu entwickeln, um eine Organisation zu schaffen, die einfach sicher ist.

Wie können CEOs die Cybersicherheit in ihren Unternehmen verbessern?

Führungskräfte, die in den letzten 2 Jahren die besten Cybersicherheit-Ergebnisse erzielt haben, sind 14-mal eher bereit, Maßnahmen zur Cybersicherheit zu unterstützen.

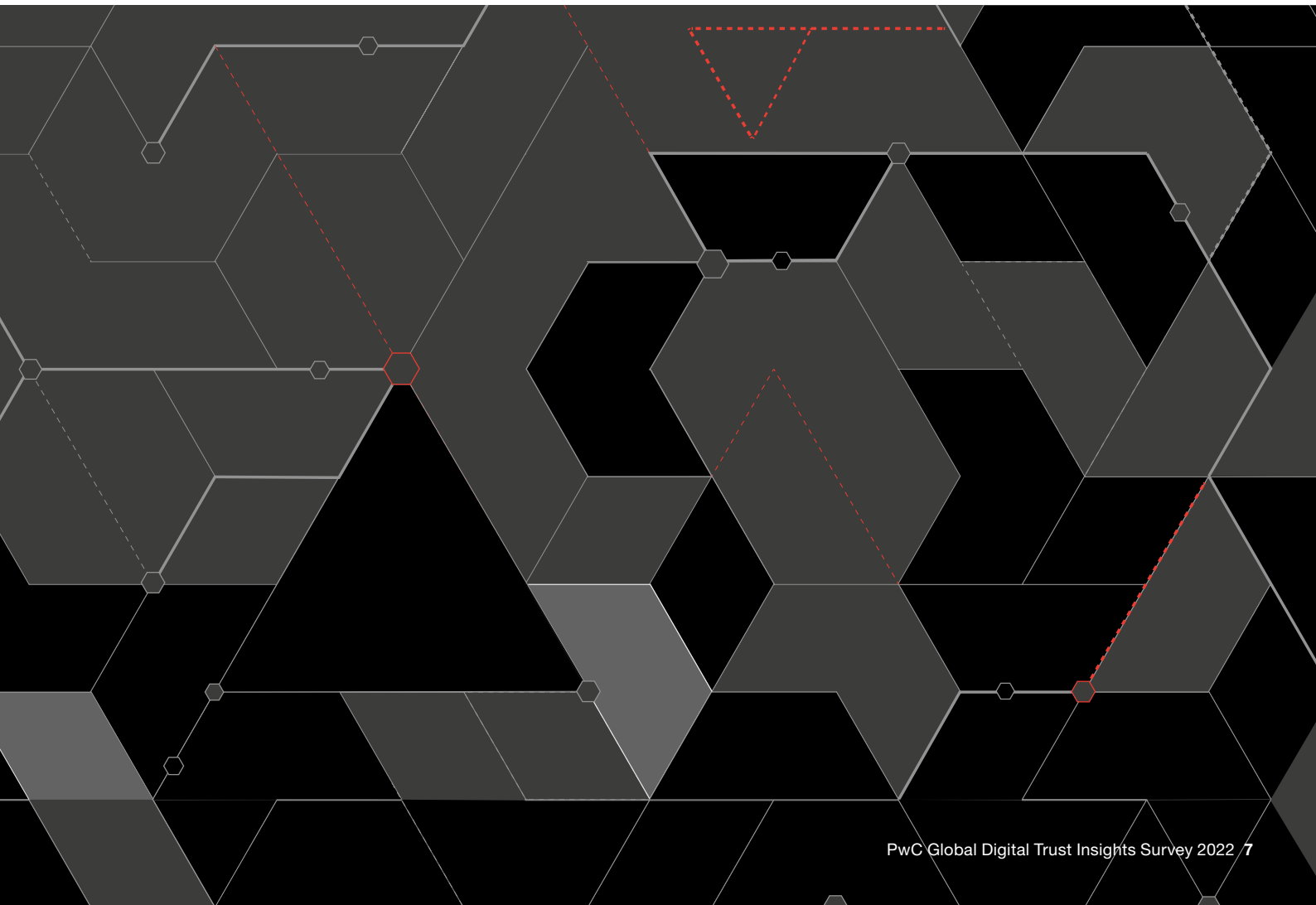
Wie können CEOs die Cyber Security stärken?

In der Studie nannten Führungskräfte Cyberbedrohungen als zweithäufigstes Risiko für die Geschäftsaussichten – nur übertroffen von Pandemien und anderen Gesundheitskrisen. In Westeuropa und Nordamerika war Cyber Security die Nummer 1.

Dabei berichten CISOs, dass ihre primäre Ansprechperson der CIO oder CTO ist. Interaktionen mit dem Chief Marketing Officer oder CFO sind deutlich seltener. Mehr als 21 Prozent der CISOs nennen den CEO als eine der drei Positionen, mit der sie am seltensten in Kontakt kommen.

Mehr Aufmerksamkeit für Cyber Security

Ein sehr wirkungsvoller Schritt für CEOs, Cybersicherheit ins Zentrum der Aufmerksamkeit zu rücken, kann eine ausdrückliche Erklärung sein, die Cybersicherheit und Datenschutz unternehmensweit zum Ziel erhebt.



Takeaways

Für CEOs

- Signalisieren Sie, wie wichtig Cyber Security für den Unternehmenserfolg und das Vertrauen der Kunden ist – nicht nur die Abwehr akuter Cyber-angriffe, sondern die Schaffung eines Cyber-Security-Mindsets in der ganzen Organisation.
- Demonstrieren Sie Vertrauen in und Unterstützung für die Arbeit des CISOs.
- Setzen Sie sich mit den Risiken in Ihren Geschäftsmodellen auseinander und ändern Sie, was geändert werden muss. Folgen Sie der Maxime: „Management bedeutet, die Dinge richtig zu tun; Führung heißt, die richtigen Dinge zu tun.“

Für CISOs

- Machen Sie sich mit der Geschäftsstrategie Ihres Unternehmens vertraut.
- Bauen Sie eine engere Beziehung zu Ihrem CEO auf und halten Sie den Dialog aufrecht, um ihm:ihr zu helfen, den Weg für einfachere, sichere Maßnahmen freizumachen.
- Entwickeln Sie die Fähigkeiten, die Sie brauchen, um in der sich entwickelnden, wachsenden Rolle des Cyberspace in der Wirtschaft erfolgreich zu sein. Und richten Sie Ihre Teams auf Business Values und Kundenvertrauen aus.

Ist Ihr Unternehmen zu komplex, um es zu sichern?

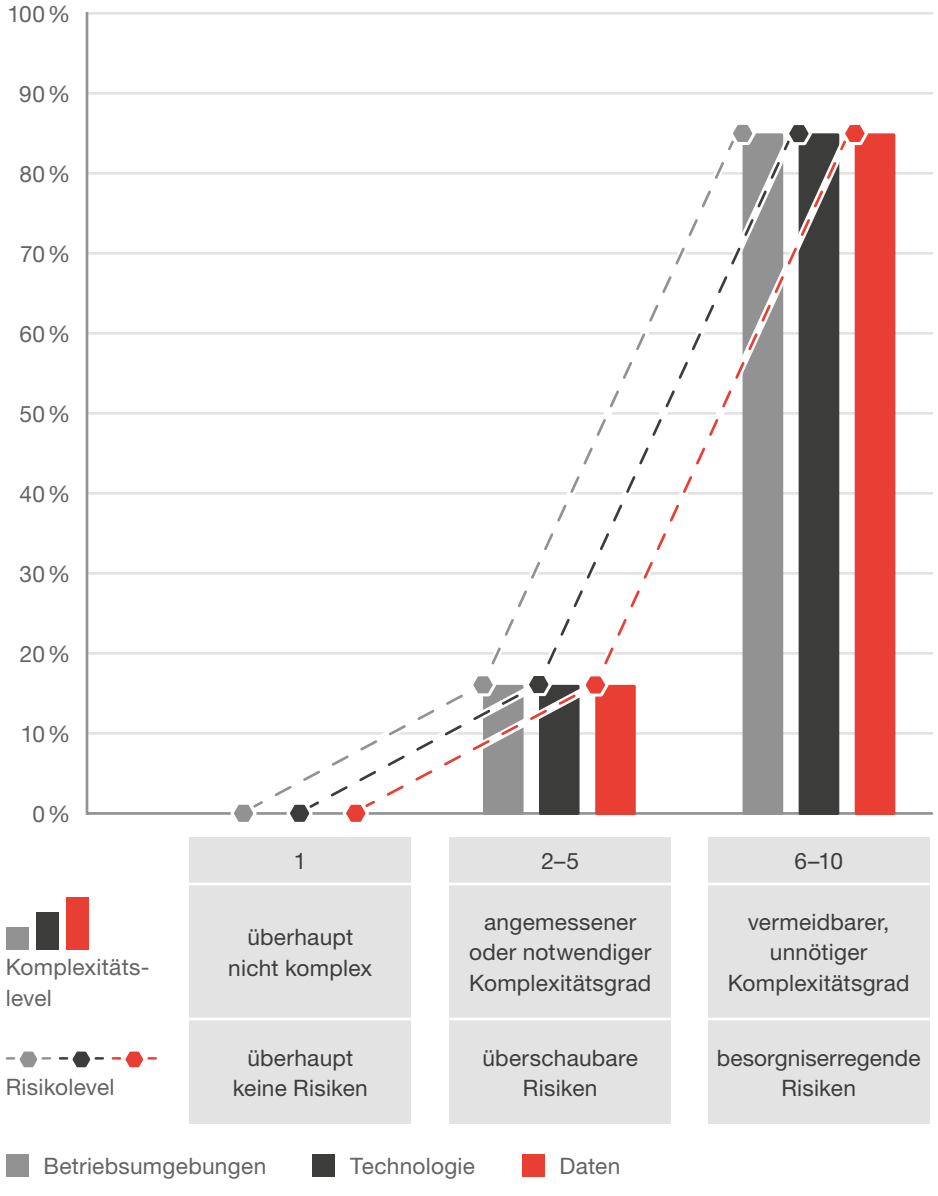
Über 80 Prozent (Global 75 Prozent) der Befragten in Deutschland geben an, dass ihre Unternehmen zu komplex sind. Unternehmen, die in den letzten 2 Jahren die besten Cybersicherheit-Ergebnisse erzielt haben, haben 5-mal eher ihre Abläufe unternehmensweit rationalisiert als andere.

Setzen Sie bewusst auf Vereinfachung

Über 80 Prozent der Führungskräfte in Deutschland geben an, dass die Komplexität in ihren Unternehmen in Bezug auf Technologie, Daten und Betriebsumgebungen zu hoch ist. Beispielsweise werden Cloud-Umgebungen von rund 77 Prozent als unnötig komplex eingestuft – noch höher liegen die Zahlen bei der Komplexität von Technologie-Anwendungen oder der Governance von Technologieinvestitionen. Die Konsequenzen der Komplexität sind: finanzielle Verluste, Unfähigkeit zur Innovation und für 50 Prozent der Befragten mangelnde Resilienz.

Abb. 4 Wie komplex sind Ihrer Meinung nach die folgenden Vorgänge in Ihrem Unternehmen auf einer Skala von 1 bis 10? Wie bedeutsam sind die Cyber- und Datenschutzrisiken aufgrund der Komplexität in diesen Bereichen Ihres Unternehmens?

Befragte, die von 1–10 bewertet haben



Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Deutschland.

Takeaways

Für Führungskräfte in den Bereichen Betrieb und Transformation
Wie sieht der Sicherheitsplan dafür aus? Wenn diese Frage jeder Führungskraft gestellt wird, die für Transformation oder eine neue Geschäftsinitiative verantwortlich ist, bedeutet das einen großen Schritt zu mehr Cybersicherheit.

Beziehen Sie den CISO sowie die Sicherheitsteams frühzeitig in die Cloud-Migration und Einführung, Fusionen und Übernahmen sowie in andere Unternehmensinitiativen ein. Dadurch vermeiden Sie überflüssige Komplexitäten – und in jeder größeren Geschäftsinitiative kann die Frage nach dem Sicherheitsplan ohne weiteres beantwortet werden.

Für CISOs und CIOs
Wagen Sie den Schritt zum Wegstreichen. Technologie und Daten neigen dazu, sich zu vermehren, ineffizient und unsicher zu werden, wenn sie sich selbst überlassen werden. Reduzieren Sie daher den Datenüberschuss mit Blick auf die Sicherheitsziele. Bewerten Sie Ihre Datenspeicher und eliminieren Sie alles, was Sie nicht mehr benötigen. Konsolidieren, liquidieren und automatisieren Sie, wo immer Sie können.

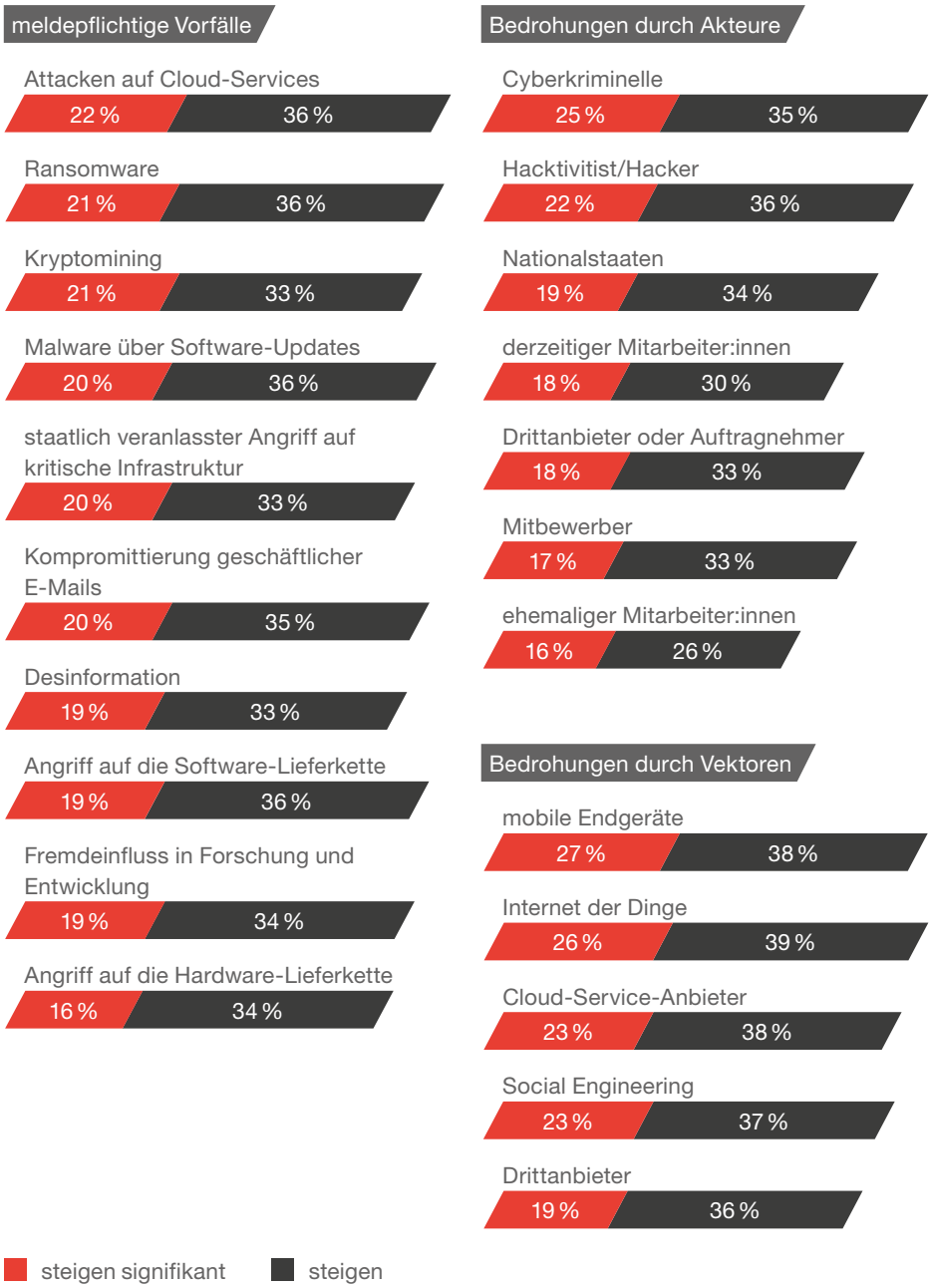
Überdenken Sie Ihre Investitionsprozesse im Bereich Technik und Cyberspace. Konzentrieren Sie sich zunächst auf die Vereinfachung des Bereichs, wo der Nutzen für die gesamte Organisation am größten ist.

Sichern Sie Ihre Organisation gegen die wichtigsten Risiken von heute und morgen ab?

Der Threat Outlook 2022

Die Führungskräfte, die für die DTI 2022 Studie befragt wurden, haben ihre Erwartung in Bezug auf relevante Cybervorfälle in den kommenden 12 Monaten geäußert: Mehr als die Hälfte der befragten Führungskräfte in Deutschland rechnet in 2022 mit mehr Angriffen – insbesondere die Bereiche Mobile, IoT und Cloud seien gefährdet. 26 Prozent rechnen mit einen signifikanten Anstieg von Cloud-Service-Angriffen, gefolgt von Ransomware (21 Prozent) und Kryptomining (21 Prozent).

Abb. 5 Der Ausblick auf die Bedrohungslage im Jahr 2022: Führungskräfte erwarten einen Anstieg der Angriffe und meldepflichtigen Vorfälle



Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Deutschland.

Takeaways

Für CFOs

- Arbeiten Sie mit dem CISO zusammen, um die Cyberstrategie mit der Geschäftsstrategie abzustimmen.

Für CISOs

- Schaffen Sie eine solide Grundlage für Data Trust: einen unternehmensweiten Zugang zu Datenmanagement, -klassifizierung, -schutz und -sparsamkeit.
- Entwickeln Sie ein ausgereiftes Risikomanagement von der Quantifizierung von Cyberrisiken bis zur Echtzeit-Berichterstattung über Cyber Security.
- Bleiben Sie nicht bei den Cyberrisiken stehen. Verknüpfen Sie die Cyberrisiken mit den allgemeinen Unternehmensrisiken und letztlich mit den Auswirkungen auf die Businessziele.
- Mit einer umfassenderen Aufstellung der Cyberrisiken können Sie erkennen, was in Ihrem Geschäftsmodell gut funktioniert und wo Sie möglicherweise vereinfachen müssen.

Wie gut kennen Sie die Cyberrisiken in ihrer Lieferkette?

Viele Unternehmen haben einen großen blinden Fleck in Bezug auf Risiken, die von Zulieferern ausgehen: Über 30 Prozent der Führungskräfte in Deutschland haben wenig bis gar kein Verständnis für die IT und Software-Risiken in ihrer Lieferkette. Ähnlich gering ist das Verständnislevel für die Risiken von Sub-Dienstleistern, Cloud und IoT-/Technologieanbietern. Nur rund ein Drittel der Befragten gibt an, dass sie das Risiko von Datenschutzverletzungen durch Dritte sehr gründlich verstehen, indem sie unternehmensweite Bewertungen durchführen.

Mehr als die Hälfte – rund 60 Prozent – haben keine Maßnahmen ergriffen, die eine nachhaltigere Wirkung auf ihr Risikomanagement für Dritte versprechen. Beispielsweise haben sie die Kriterien für die Auswahl von Zulieferern nicht verfeinert, die Verträge nicht umgeschrieben und keine strenge Prüfung bei der Auswahl durchgeführt.

Abb. 6 Hat Ihr Unternehmen in den letzten 12 Monaten eine der folgenden Maßnahmen ergriffen, um die Risiken von Drittanbietern oder Lieferanten in Ihrem Ökosystem zu minimieren?

Quelle: PwC „Global Digital Trust Insights 2022“, Ergebnisse Deutschland.

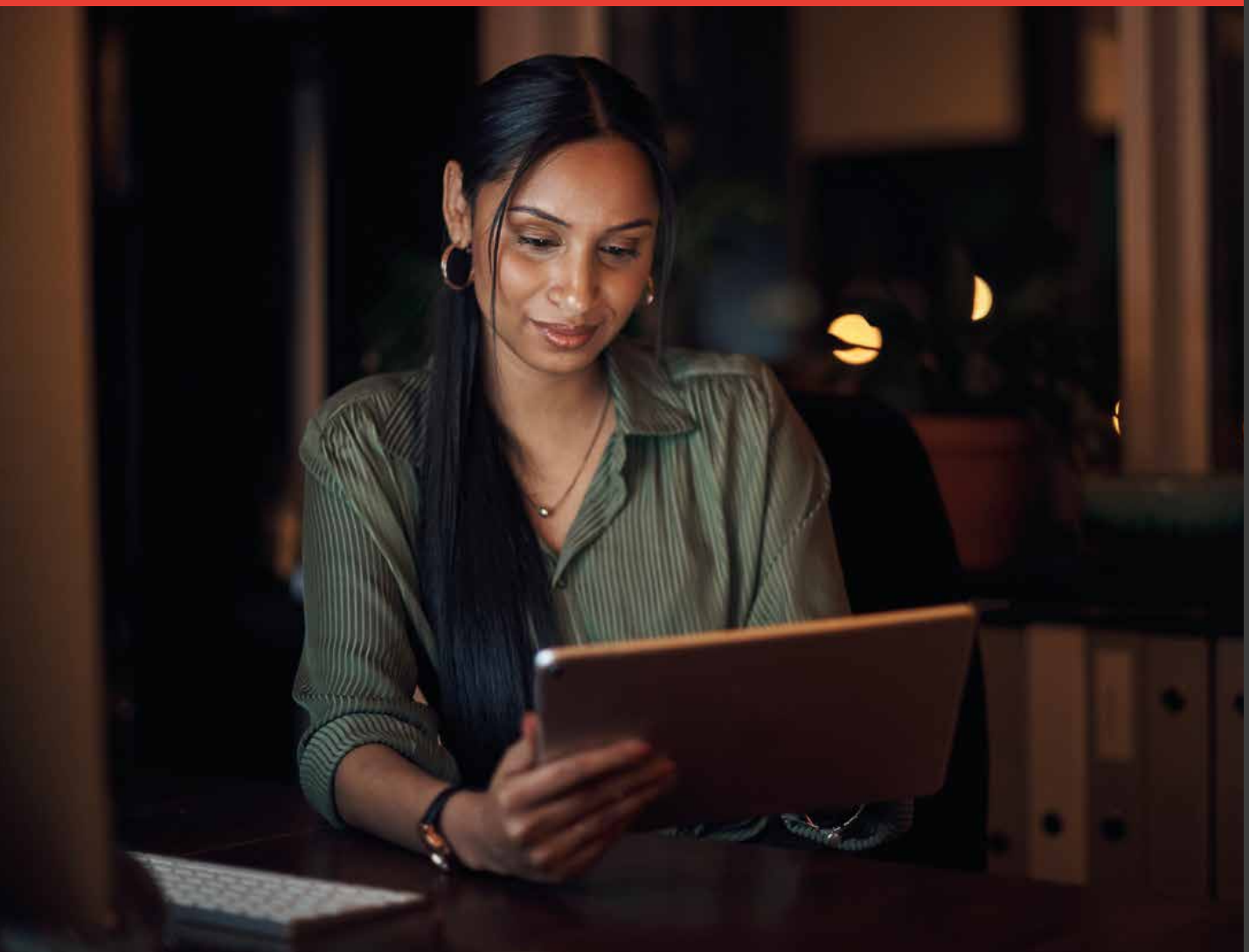
Takeaways

Für COOs und Führungskräfte im Bereich Lieferkettenmanagement

- Erstellen Sie eine Übersicht über Ihr System, insbesondere über Ihre kritischsten Vernetzungen, und analysieren Sie die Cyber Security bei Drittanbietern, um die schwächsten Glieder Ihrer Lieferkette zu finden.
- Überprüfen Sie Softwareanbieter mithilfe von Good-Practice-Standards, die sie vorgeben. Diese Vorgaben sollten sowohl für Software und Anwendungen als auch für Netzwerkgeräte und Verhaltensregeln gelten.
- Nachdem Sie die Risiken in Bezug auf Dritte und die Lieferkette genauer untersucht haben, sollten Sie nach Möglichkeiten suchen, Ihre Vernetzungen zu vereinfachen.

Für CROs und CISOs

- Richten Sie eine verantwortliche Position für das Risikomanagement von Drittanbietern ein, um alle entsprechenden Aktivitäten an einer Stelle zu koordinieren.
- Verstärken Sie Data-Trust-Prozesse. Daten sind das Ziel der meisten Angriffe auf Partner und Lieferanten. Data Trust und ein gutes Risk Management gehören zusammen.
- Berichten Sie regelmäßig dem Vorstand über Cyber- und Geschäftsrisiken, die von Partnern und Lieferanten ausgehen können.



Über die Studie

Im Rahmen der Global Digital Trust Insights 2022 wurden zwischen Juli und August 2021 insgesamt 3.602 Führungskräfte (CEOs, Corporate Directors, CFOs, CISOs, CIOs und C-Suite-Verantwortliche) aus den Bereichen Wirtschaft, Technologie und Sicherheit zur Entwicklung und Zukunft von Cybersicherheit befragt. 33 Prozent der jeweiligen Unternehmen sind in Westeuropa ansässig, davon 258 in Deutschland, gefolgt von Nordamerika (26 %), Asien-Pazifik (18 %), Lateinamerika (10 %), Osteuropa (4 %), Naher Osten (4 %) und Afrika (4 %).

62 Prozent der Befragten sind Führungskräfte in Unternehmen mit einem Umsatz von 1 Milliarde Dollar und mehr, 33 Prozent in Betrieben mit einem Umsatz von 10 Milliarden Dollar und mehr. Die Teilnehmenden sind in einer Vielzahl von Branchen tätig: Technik, Medien, Telekommunikation (23 %), industrielle Fertigung (22 %), Finanzdienstleistungen (20 %), Einzelhandels- und Verbrauchermärkte (16 %), Energie, Versorgungsunternehmen und Ressourcen (8 %), Gesundheit (7 %) und öffentlicher Dienst (3 %).

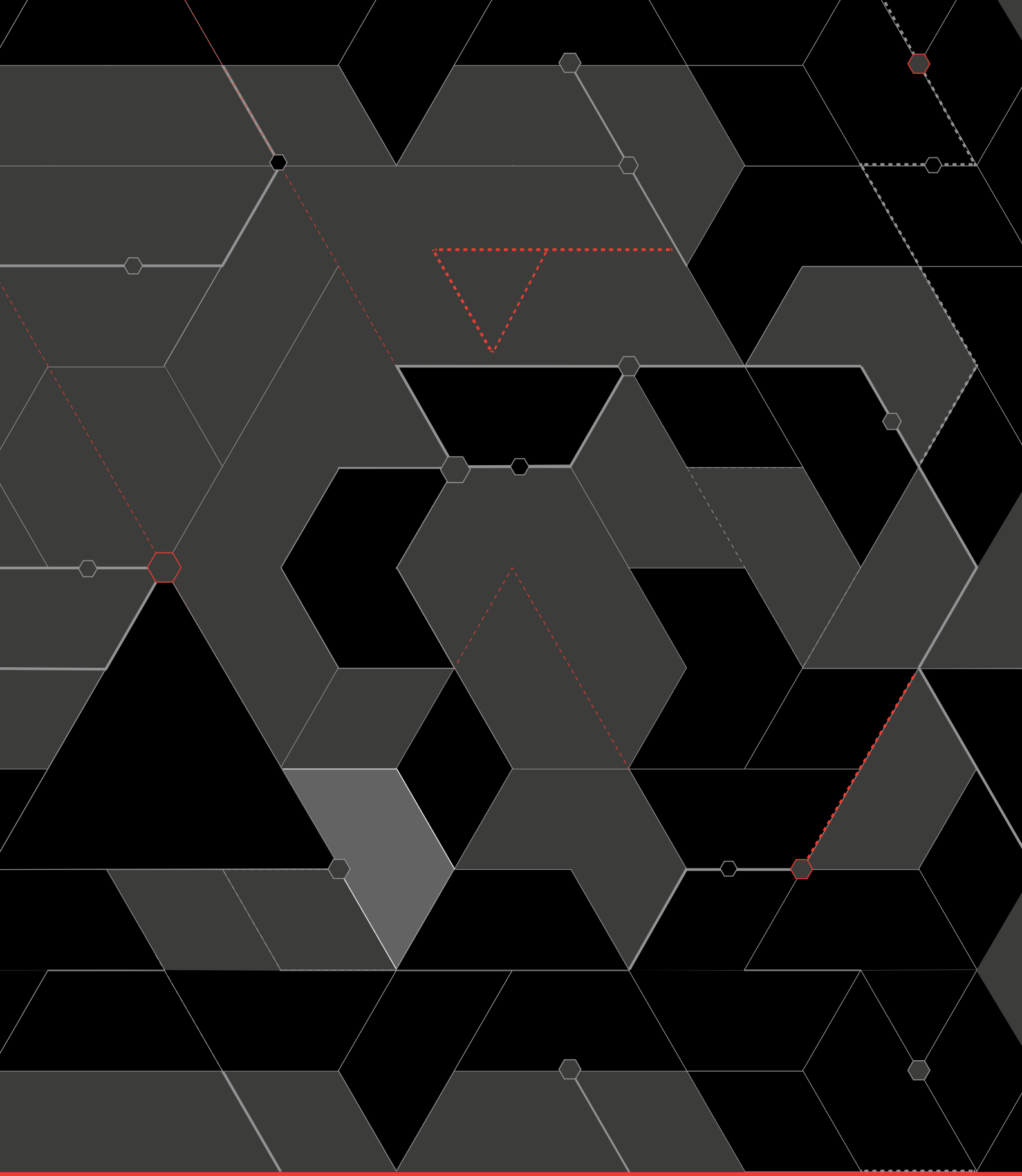
Kontaktieren Sie uns hier:

https://www.pwc.de/cyber-security-beratung

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 155 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Rund 12.000 engagierte Menschen an 21 Standorten. 2,3 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.



www.pwc.de