Willis Towers Watson

Cyber-Sicherheit

Das ganze Bild im Blick

Cyber-sicher in die Zukunft

Vielleicht ebnet in diesem Moment ein Mitarbeiter Ihres Unternehmens Cyber-Kriminellen den Weg in Ihr IT-System – dazu reicht ein Mausklick auf den infizierten Anhang einer E-Mail. Sensible Daten sind dann genauso gefährdet wie digitale Prozesse, digital gesteuerte Anlagen oder die Online-Interaktion mit Kunden.

Cyber-Attacken können in vielfältigen Varianten jedes Unternehmen treffen. Und die Kosten infolge einer erfolgreichen Attacke gehen oft in die Millionen. Vor allem Betriebs- und Lieferketten-Unterbrechungen sowie von Datendiebstählen spiegeln sich in der Unternehmensbilanz schmerzhaft wider.

Das Problem: Viele Unternehmen wissen nicht genau, welchen Cyber-Risiken sie ausgesetzt sind und wie gravierend sich diese Risiken auswirken können. Sie haben dann auch kaum eine Chance, sich angemessen zu schützen und bei Bedarf schnell und gezielt zu reagieren.

Willis Towers Watson hilft Ihnen, für Klarheit, Sicherheit und Handlungsfähigkeit zu sorgen. Als weltweit führende Experten in den Bereichen HR-Management, Risikomanagement und Broking überschauen wir dabei alle relevanten Themen.

Wir identifizieren mit Ihnen die Risiken, die von einem Fehlverhalten Ihrer Mitarbeiter und von Schwachstellen Ihres IT-Systems ausgehen. Und wir klären, zu welchen finanziellen Verlusten diese Risiken im Falle eines Falles führen können.

Mit diesem Bild vor Augen entwickeln wir zum einen HR- und IT-Lösungen, die Ihre Risiken reduzieren. Zum anderen erarbeiten wir mit Ihnen Versicherungslösungen, die Ihr Unternehmen vor potenziellen finanziellen Schäden schützen. Dazu nutzen wir unsere umfassende Erfahrung, Wissen und modernste analytische Tools.

Nehmen Sie mit uns die Cyber-kritischen Themen „Mitarbeiter“, „Kapital“ und „Technologie“ im Rahmen einer durchdachten Risiko-Management-Strategie ganzheitlich in den Blick. Und geben Sie so Ihrem Unternehmen die Sicherheit, die es auf seinem Weg in die Zukunft braucht.

Marcus Kuhn, LL.M.
Manager Finex

Cyber-Sicherheit

Das ganze Bild im Blick

Inhalt

Bedrohungslage
Die generellen Risiken verstehen

Wer das Thema „Cyber-Sicherheit“ auf die leichte Schulter nimmt, verkennt die Lage: Cyber-Kriminelle sind sehr aktiv – zum Schaden vieler Unternehmen. Verschaffen Sie sich mit uns einen Überblick.

Milliarden-Verluste für die deutsche Wirtschaft

Machen Sie sich kurz bewusst, wie viel Digitalisierung in Ihrem Unternehmen steckt: Kunden- und Mitarbeiterdaten, Informationen zu Marktinitiativen und zu neuen Produkten, digitale Wertschöpfungs- und Kommunikationsprozesse. Die Reihe ließe sich leicht fortsetzen – ohne Digitalisierung läuft heute wenig.

Wer Ihre digitalen Prozesse stört oder sich Zugang zu sensiblen Daten verschafft, kann Ihrem Unternehmen schaden, sogar sehr. Der Branchenverband Bitkom nennt in einer Studie aus dem Jahr 2018 eine alarmierende Zahl: In einem zweijährigen Erhebungszeitraum verloren Unternehmen in Deutschland durch digitale Wirtschaftsspionage, Sabotage und Datendiebstahl rund 43 Mrd. Euro.[1]

Es kann jedes Unternehmen treffen

Zu Buche schlagen etwa Verluste durch Reputationsschäden und Verletzungen gewerblicher Schutzrechte (z. B. Patentrechtsverletzungen), durch sabotierte Informations- und Produktionssysteme und Betriebsabläufe, Kosten für Ermittlungen, Rechtsstreitigkeiten und Aufwendungen für datenschutzrechtliche Maßnahmen.

Sieben von zehn Unternehmen haben erkannt, dass sie Opfer von Cyber-Angriffen waren, so ein weiteres Ergebnis der Studie. Doch die Dunkelziffer ist hoch. Kein Unternehmen sollte sich in Sicherheit wiegen. Und immer weniger tun dies auch. Das Thema „Cyber-Sicherheit“ ist angekommen.

Cyber-Kriminelle sind kompetent und kreativ

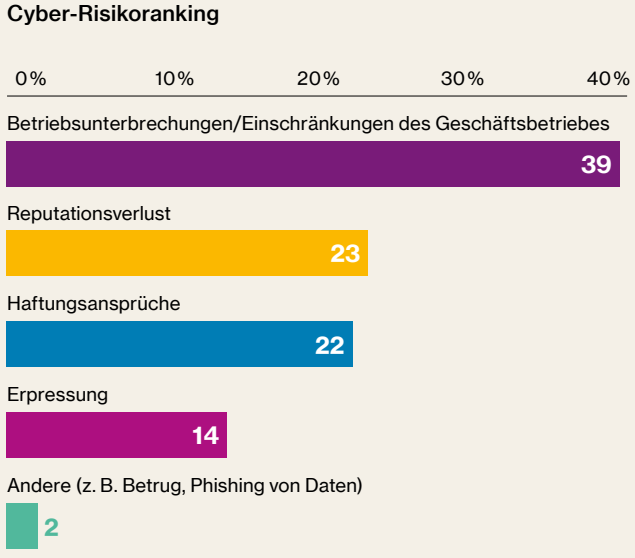
Der Täterkreis ist dabei recht vielfältig; er umfasst ehemalige Mitarbeiter und Hobby-Hacker genauso wie Wettbewerber, organisierte Banden und ausländische Nachrichtendienste. Sie sabotieren, spionieren, stehlen Daten und erpressen.

Und viele Cyber-Kriminelle sind sehr kompetent: Sie bewegen zum Beispiel Mitarbeiter mit geschickt gefälschten E-Mails dazu, infizierte Anhänge zu öffnen oder auf infizierte Websites zu gehen. Sie überlasten Server und IT-Infrastrukturen mit massiven Anfragen, hacken kritische Datenbanken oder spähen ihre Opfer lange unbemerkt aus. Ihre kriminelle Kreativität kennt keine Grenzen.

Internationale Schadenfälle bieten Transparenz

Diese generelle Bedrohungslage sollte in unserer vernetzten digitalen Wirtschaftswelt jedes Unternehmen kennen. Gefragt ist umfassende Transparenz. Wilis Towers Watson bietet sie Ihnen auf Basis klarer Fakten.

Denn die ernsten Gefahren kennen wir aus erster Hand durch unsere nationale und internationale Erfahrung mit zahlreichen Schadenfällen. Kritische Szenarien und Trends, die für Ihre Branche relevant sind, können wir Ihnen auch IT-basiert veranschaulichen – damit Sie sehen, worum es geht: um die Zukunft Ihres Unternehmens!



Als Folge von Cyber-Attacken fürchten Unternehmen vor allem Betriebsunterbrechungen (Willis Towers Watson Pulse Survey Cyber 2018).

1 Bitkom: Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Indsutrie. Studienbericht 2018

Risikoprofil
Relevante Risiken erkennen und bewerten

Nur wer seine Risiken kennt, kann sich davor schützen. Entscheidend ist Ihr konkretes Risikoprofil. Wir erarbeiten es „hands on“ mit Ihnen. Dabei helfen uns modernste Tools und unsere umfassende Expertise.

Das ganze Bild entscheidet

Das Thema „Cyber-Sicherheit“ ist komplex: Die meisten Schadenfälle resultieren aus einem Fehlverhalten der Mitarbeiter. Viele IT-Systeme entsprechen nicht den gebotenen Sicherheitsstandards. Und welche Cyber-Vorfälle zu welchen Schäden und Kosten führen können, ist vielen Unternehmen unklar. Die Risikostrategie kann so nur im Vagen bleiben.

Ihre Lage betrachten und bewerten wir deshalb aus einer umfassenden Perspektive. Sie nimmt Ihre Mitarbeiter genauso in den Blick wie Ihr IT-System und die finanziellen Folgen potenzieller Cyber-Attacken. Nur das ganze Bild ist aussagekräftig.

Gefahren benennen – mögliche Verluste beziffern

Dieses Bild entwerfen wir mit Ihnen gemeinsam – damit Ihnen Ihre wesentlichen Risiken und die jeweils potenziellen finanziellen und bilanziellen Folgen transparent werden. Dazu gehen wir mit Ihnen einen praxisbewährten Weg:

- Als erstes verschaffen wir uns einen Überblick über den Status quo: Mit welchen Risiken und Schäden wurden Sie bereits konfrontiert? Wo liegen Ihre besonderen Herausforderungen?
- Dann können wir analysieren, wie Cyber-sicher Ihre Unternehmenskultur ist. Welche Faktoren begünstigen ein Fehlverhalten Ihrer Mitarbeiter? Welche Mitarbeitergruppen sind besonders kritisch?
- Bei Bedarf identifizieren wir auch mit ausgewählten Partnern und eigenen Mitteln die Sicherheitslücken Ihres IT-Systems: Wo können Cyber-Kriminelle eindringen? Welche Prozesse und Schnittstellen sind gefährdet?
- Und wir quantifizieren die finanziellen Verluste, die sich etwa aus Betriebsunterbrechungen und Datenschutzverletzungen ergeben können. Wie sehen relevante Schadenszenarien aus? Welche Kosten sind damit verbunden?

Gut informiert handlungsfähig werden

Wenn Sie mit uns Ihr Cyber-Risikoprofil erarbeiten, gewinnen Sie ein objektives Bild im Rahmen der entscheidenden Themen „Mitarbeiter“, „Kapital“ und „Technologie“. Sie erkennen Ihre unternehmensspezifischen Risiken und zu welchen finanziellen Verlusten sie führen können.

Mit unserer internationalen Expertise in den Bereichen HR-Management, Risikomanagement und Broking und unseren marktführenden IT-Tools helfen wir Ihnen, Ihre Risiken so zu analysieren und zu bewerten, dass Sie auf einer belastbaren Faktenbasis in Sachen Cyber-Sicherheit handlungsfähig werden.

Risiko-Landkarte

Schutz
Passgenaue Lösungen finden

Das beste Wissen um die eigenen Risiken ist wertlos, wenn man nichts aus diesem Wissen macht. Wir helfen Ihnen, den entscheidenden Schritt zu wirkungsvollen Lösungen zu gehen.

Vom Wissen zum Handeln

Wenn Sie Ihr Risikoprofil mit uns erarbeitet haben, heißt es: Handeln! Dabei geht es um drei zentrale Fragen: Welche Risiken lassen sich minimieren? Welche Verluste, die mit verbleibenden Risiken verbunden sind, können Sie selbst tragen? Und welchen Verlusten sollten Sie mit Versicherungslösungen begegnen?

Die technischen Sicherheitslücken können wir mit Ihren IT-Experten und ausgewählten IT-Partnern angehen. Allerdings sind Cyber-Kriminelle oft einen Schritt voraus. Ein hohes Sicherheitsniveau erfordert deshalb auch eine sensible und geschulte Mannschaft und eine individuelle finanzielle Risikostrategie.

Risiko Mitarbeiter

Die eigenen Mitarbeiter sind das größte Risiko bei Cyber-Angriffen, wie auch eine internationale Studie von Willis Towers Watson belegt.[2] Denn die Arbeitswelt wird immer digitaler. Und vielen Mitarbeitern fehlt das Bewusstsein für die Risiken aus dem Cyber-Raum.

Sie verlassen sich auf Virenschutzprogramme und Firewalls oder machen sich schlicht keine Gedanken darüber, was sie mit einem Mausklick auslösen können. Kurz: Die Kultur vieler Unternehmen ist nicht auf das Thema „Cyber-Sicherheit“ ausgerichtet. Und dies nutzen Cyber-Kriminelle aus.

Eine Cyber-Kultur etablieren

Mit unserer HR-Management- und Risiko-Management-Expertise helfen wir Ihnen nicht nur, die Schwachstellen Ihrer Unternehmenskultur zu identifizieren. Wir stehen Ihnen auch dabei zur Seite, diese Schwachstellen zu beheben.

Welche Mitarbeitergruppen in Ihren Reihen dabei besonders kritisch sind, ermitteln wir anhand unserer internationalen Erfahrung mit Cyber-Vorfällen und mit maßgeschneiderten Culture Surveys in Ihrem Unternehmen.

Um das Cyber-Bewusstsein dieser Gruppen zu stärken, entwickeln wir gezielte Maßnahmen – dazu gehören Trainings zum Umgang mit E-Mails und mit Passwörtern, Schulungen rund um die Datenschutzgrundverordnung (DSGVO) oder Kommunikationsstrategien, die Ihre Mitarbeiter aufmerksam machen.

Für Cyber-kompetente Mitarbeiter sorgen

Entscheidend ist jedoch auch, dass Ihre Mitarbeiter – gerade in Cyber-kritischen Bereichen – über die richtigen Kompetenzen verfügen. Neben einem Kulturwandel kommt es deshalb auf eine Cyber-affine HR-Management-Agenda an.

Dazu identifizieren wir, welche Kompetenzen Ihre Mitarbeiter mit Blick auf welche Cyber-Risiken brauchen und welche individuellen Lücken sie noch haben. Dieses Bild ist die Basis, um Ihre Mitarbeiter gezielt Cyber-fit zu machen.

Im Rahmen dieser Cyber-Readiness-Diagnose können wir zudem ein Kompetenzmodell mit Ihnen entwickeln, das genau auf Ihr Risikoprofil abgestimmt ist. Dieses Modell hilft dabei, Cyber-Kompetenzen in Ihr gesamtes Talentmanagement zu integrieren – vom Recruiting bis zur Personalentwicklung.

Den Versicherungsschutz modellieren

Doch bei aller Vorsicht: Im Cyber-Raum ist kein Unternehmen völlig sicher. Gefragt ist deshalb auch ein ausreichender Versicherungsschutz. Aber welche Versicherungslösungen sind für Sie die richtigen? Um diese Frage zu beantworten und eine fundierte Risikostrategie zu entwickeln, modellieren wir mit Blick auf Ihr Risikoprofil mögliche Szenarien, die zeigen,

- welche Risiken mit welcher Wahrscheinlichkeit eintreten und wie gravierend sie sich finanziell auswirken können,
- und welche möglichen Verluste sie selbst tragen können, welche Sie mit Versicherungen absichern sollten und welche Selbstbehalte und Deckungssummen dabei für Sie die besten sind.

2 Willis Towers Watson 2017 Cyber Risk Survey

Schutz und Kosten gut ausbalancieren

Mit diesem Zielbild vor Augen bewerten wir Ihr Versicherungsportfolio. Die Herausforderung: In Haftpflichtversicherungen oder Versicherungen anderer Sparten sind Cyber-Risiken oft nicht explizit genannt oder nur schwammig adressiert. Oder sie sind gut verankert, jedoch gleichzeitig über eine Cyber-Versicherung abgedeckt.

Im Zuge einer gesamtwirtschaftlichen Betrachtung muss hier über alle Sparten die richtige Balance von Schutz und Kosten gefunden werden. Als neutraler Versicherungsmakler finden wir für Sie eine passende Lösung.

Dazu gehört eine Cyber-Versicherung: Maßgeschneidert gestaltet deckt sie alle relevanten Kosten, die aus Betriebsunterbrechungen und Datenschutzverletzungen entstehen. Wir richten sie im Kontext Ihrer anderen Versicherungen so aus, dass Sie auf der sicheren und wirtschaftlichen Seite sind.

Silent Cyber: das unterschätzte Risiko

Wer sich mit seinen bestehenden Versicherungen auch bei Cyber-Angriffen gut geschützt wähnt, sollte die Versicherungsbedingungen noch einmal genau lesen. Bieten sie wirklich den gewünschten Schutz? Zwei Beispiele:

- Durch eine Cyber-Attacke auf ein Kontrollsystem wird eine Produktionsanlage überhitzt; die Anlage wird zerstört und ein Feuer sorgt für weitere Schäden.
- Eingeschleuste Malware lässt einen voll besetzten digital gesteuerten Aufzug über mehrere Etagen abstürzen – auch mit Folgen für Leib und Leben.

Begleichen die Versicherungen die finanziellen Schäden und Forderungen? Hier kommt es auf das Bedingungswerk und den Bedingungsumfang an. Werden Cyber-Angriffe nicht explizit genannt, könnten sie eventuell „mitgemeint“ sein, aber eben nur eventuell. Und wird auf Cyber-Attacken verwiesen, geschieht dies oft so schwammig, dass längere Diskussionen mit dem Versicherer anstehen, bei ungewissem Ausgang. Sorgen Sie also für Klarheit.

D&O-Versicherungen: Cyber-Risiken sind „Board“-Risiken

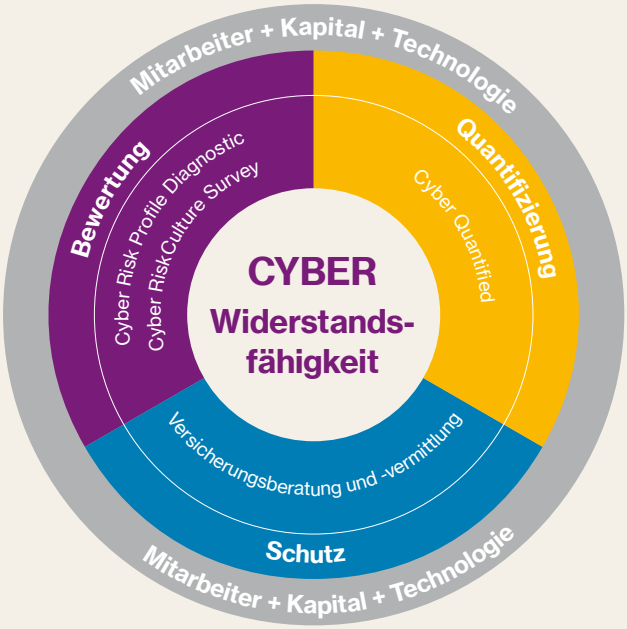
Ein Cyber-Angriff kann schnell zu immensen Verlusten führen – etwa zu Umsatzeinbußen bei Betriebsunterbrechungen, zu Ansprüchen Dritter bei Datenschutzverletzungen, zu Kosten, um alles wieder zum Laufen zu bringen und zu Aufwendungen für Forensiker und juristische Verfahren.

Vorstände und Geschäftsführer müssen dafür sorgen, dass diese finanziellen Verluste nicht zu Lasten ihres Unternehmens gehen: Sie stehen in der Haftung und tun deshalb gut daran, für eine leistungsstarke Cyber-Versicherung zu sorgen.

Allerdings decken Cyber-Versicherungen nicht immer alle Verluste ab. Zudem schauen die Versicherer genau hin, ob Vorstände und Geschäftsführer ihrer Sorgfaltspflicht Genüge getan haben. Außerdem sind Aufsichtsräte verpflichtet, gegen ihre Vorstände vorzugehen, wenn eine Haftung hinreichend wahrscheinlich ist.

Selbst wenn eine Cyber-Versicherung vorliegt, sollten Vorstände und Geschäftsführer deshalb eine D&O-Versicherung abschließen. Sie springt sogar bei grob fahrlässigem Verhalten ein. Und wer kann schon genau dokumentieren, dass er alles getan hat, um sein Unternehmen zu schützen?

Unser ganzheitlicher Ansatz beim Risikotransfer



Krisenmanagement
Schnell erfolgreich handeln

Cyber-Attacken können jedes Unternehmen treffen. Weil dann Zeit Geld ist, heißt es sofort das Richtige tun. Wir entwickeln mit Ihnen dazu einen Notfallplan und begleiten Sie im Falle eines Falles als konstruktiver Partner.

Gute Vorbereitung entscheidet

Immer wieder läuten in Unternehmen die Alarmglocken: Blockierte Rechner, überlastete Server, verschlüsselte Daten, sabotierte Produktionsanlagen, abgeflossene Kundendaten und andere Vorfälle sorgen für Hektik. Es kommt jedoch darauf an, mit kühlem Kopf schnell und gezielt zu handeln. Deshalb sollten Sie sich und Ihre Mitarbeiter mit einem Notfallplan auf Cyber-Attacken gut vorbereiten.

An alles Wichtige denken

Wir entwickeln mit Ihnen einen individuellen Notfallplan und wir helfen Ihnen, bei Bedarf das Richtige zu tun. Generell geht es um folgende To-dos:

- Die Lage klären: Melden Sie einen kritischen Vorfall umgehend Ihrem Versicherungspartner oder eingebundenen Dienstleistern. Spezialisierte Experten und Ihr IT-Team können dann zügig ermitteln, welche Form die Attacke hat, welche Daten und Systeme betroffen sind und welche Schäden daraus resultieren.
- Die Schäden minimieren: Ist die Lage geklärt, geht es darum, die Schäden zu beheben oder zumindest so klein wie möglich zu halten – also zum Beispiel Datenlecks zu schließen, schädliche Software zu neutralisieren und wieder für einen Normalbetrieb zu sorgen.
- Den Verlauf dokumentieren: Behörden und Versicherungen prüfen, ob Sie Ihrer Sorgfaltspflicht gefolgt sind. Dokumentieren Sie also genau, was passiert ist und was Sie unternommen haben, um die Schäden zu begrenzen.
- Meldepflichten einhalten: Wenn Schäden Dritte betreffen, müssen Sie schnell für Transparenz sorgen. Datenpannen sind zum Beispiel innerhalb von 72 Stunden der zuständigen Datenschutzbehörde zu melden. Klären Sie schon jetzt, welchen Meldepflichten Ihr Unternehmen in welchen Fällen unterliegt.
- Mit Stakeholdern kommunizieren: Bei gravierenden Fällen wollen Kunden, Mitarbeiter und die Öffentlichkeit wissen, was passiert ist. Halten Sie alle Stakeholder auf dem Laufenden. Besprechen Sie zudem mit Anwälten, welche Ansprüche Geschädigte gegen Sie haben könnten. Und klären Sie mit Ihrem Makler und Versicherer, welche Schäden und Verluste abgedeckt sind.

Finanzielle Verluste reduzieren

Wir bereiten Sie auf Cyber-Notfälle vor. Wir stehen Ihnen in einer Cyber-Krise mit Rat und Tat zur Seite, vor allem, wenn es darum geht, Ihre Forderungen gegenüber Ihrer Versicherung geltend zu machen. Und wir helfen Ihnen, aus den Erfahrungen mit einem Cyber-Vorfall zu lernen.

Als internationale Experten in Sachen Risikomanagement und Cyber-Sicherheit bieten wir Ihnen mit unseren Partnern alle Kompetenzen, auf die es bei einer Cyber-Attacke ankommt. Gemeinsam können wir so Ihre finanziellen Verluste auf ein Minimum reduzieren.

Typische Cyber-Vorfälle: Schäden und Regulierung

Willis Towers Watson hat weltweit bereits über 1.300 Schadenfälle nach Cyber-Angriffen begleitet – ein typisches Beispiel:

Datenschutzverletzung – Gesamtkosten über 100 Mio. Euro:
Ein Cyber-Angriff hat die Daten von zig Millionen bestehender und ehemaliger Kunden des Versicherten gefährdet. Die Attacke wurde entdeckt, als ein Mitarbeiter feststellte, dass eine Datenbankabfrage mit seinen Zugangsdaten erfolgt war. Der Mitarbeiter stoppte die Anfrage und informierte die IT-Sicherheitsabteilung. Der Versicherte schaltete mehrere Cyber-Experten ein, um den Schaden zu begrenzen. Die Versicherung hat alle Kosten im Rahmen des Versicherungsvertrags erstattet.

Zusammenarbeit
Gemeinsam den besten Weg gehen

Cyber-Sicherheit ist ein komplexes Thema. Wir helfen Ihnen, diese Komplexität zuverlässig zu beherrschen – individuell, analytisch durchdacht und kreativ.

Passend zu Ihrem Unternehmen

Ihr Unternehmen ist einmalig. Seine strategische Agenda und die Unternehmenskultur, die Mitarbeiter, die sich für die gemeinsamen Ziele engagieren, sowie die Strukturen, Prozesse und Systeme machen es unverwechselbar.

Diese Individualität bedeutet auch, dass Ihr Unternehmen charakteristischen Cyber-Risiken ausgesetzt ist und die potenziellen finanziellen Verluste im Falle eines Falles sehr spezifisch sind.

Deshalb brauchen Sie Lösungen, die genau zu Ihrem Unternehmen passen. Wir erarbeiten diese Lösungen gemeinsam mit Ihnen – mit einem ganzheitlichen Blick auf Ihre Mitarbeiter, Ihr IT-System und Ihre finanzielle Risikostrategie.

Ein vielfältiges Team an Ihrer Seite

Dafür steht unser Cyber-Team in Deutschland, das weltweit mit den Cyber-Sicherheits-Experten von Willis Towers Watson und mit erstklassigen Dienstleistern vernetzt ist. Ganz nach Ihrem Bedarf engagieren sich für Sie HR- und Risikomanagement-Profis und Versicherungsmakler genauso wie IT-Spezialisten, Forensiker und Anwälte.

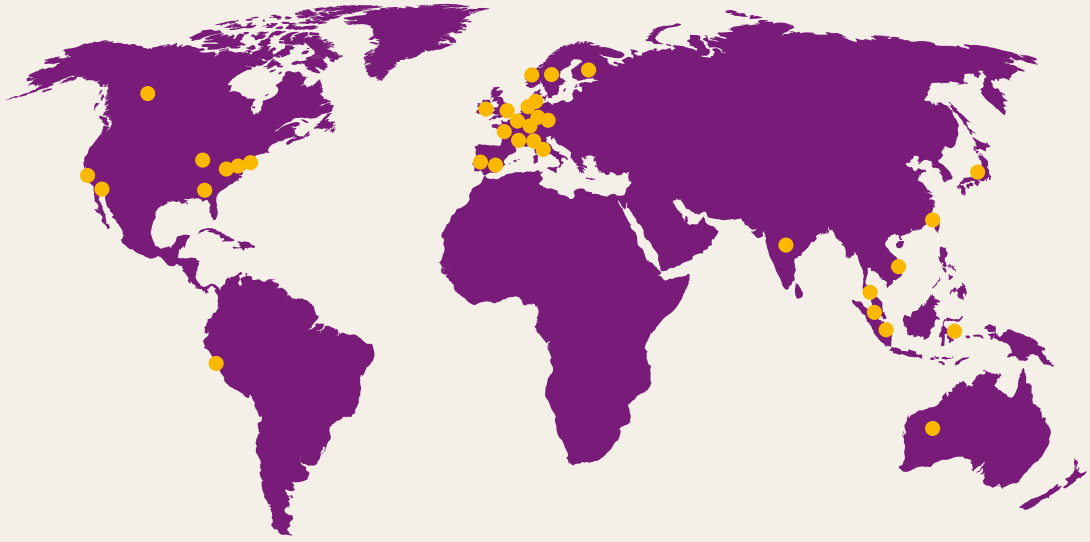
Sie profitieren von unserer Expertise und internationalen Erfahrung mit Schadenfällen genauso wie von unseren analytischen IT-Tools, die Ihre Entscheidungen in Sachen Cyber-Sicherheit auf eine objektive Basis stellen.

Neue Fragen brauchen neue Antworten

Zudem suchen wir kreativ auch nach innovativen Wegen, damit Sie Ihre Risiken beherrschen können. Denn die digitale Welt ist in Bewegung. Themen wie Big Data, Künstliche Intelligenz oder das Internet der Dinge führen zu immer wieder neuen Bedrohungslagen. Deshalb kommt es stets auf frische Ideen an.

Ihr Unternehmen braucht Sicherheit, um erfolgreich in unseren digitalen Zeiten handeln zu können. Dazu machen wir unser gesamtes Know-how und Do-how gerne mit Ihnen gemeinsam produktiv.

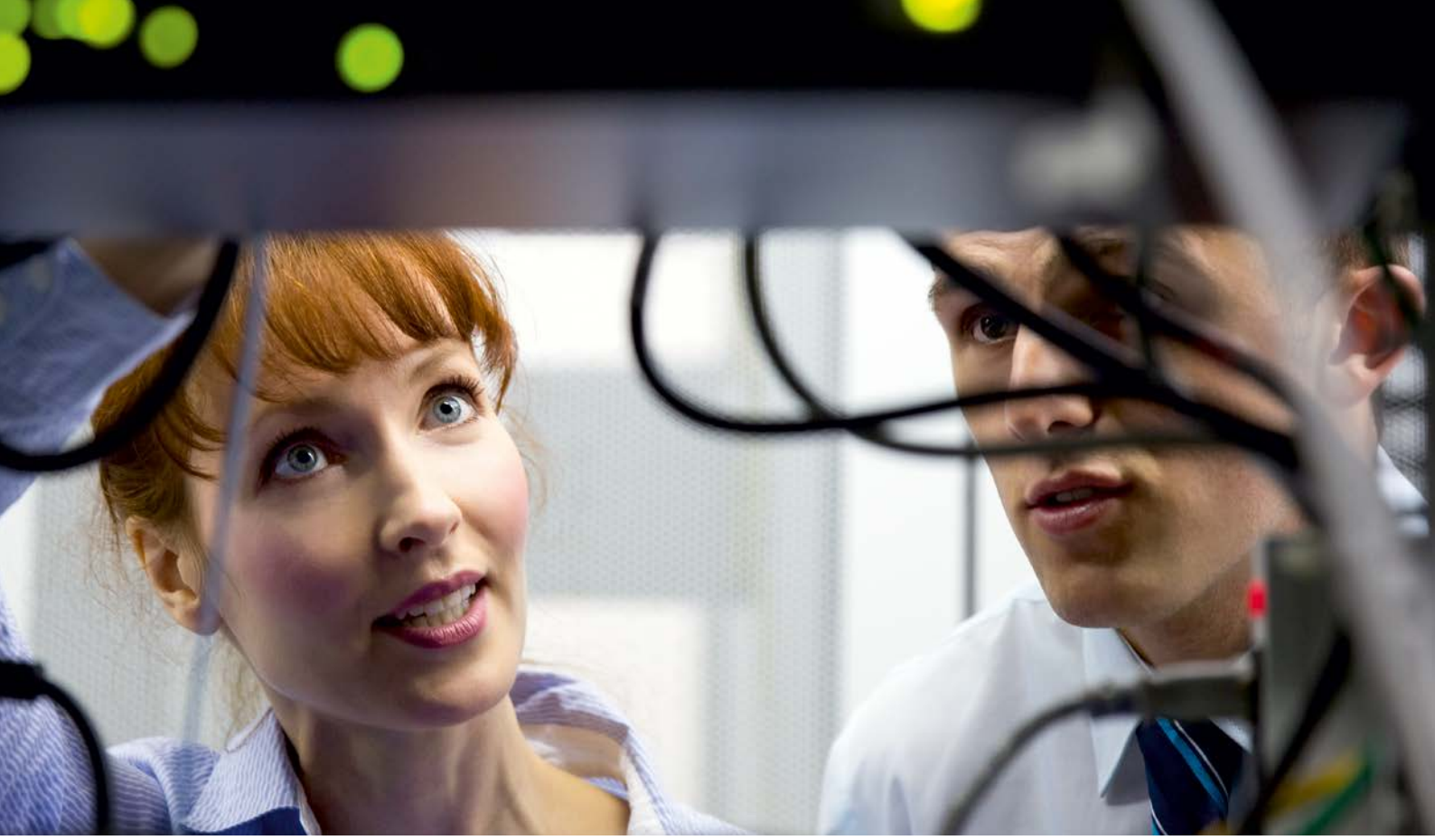
Globale Präsenz, Betreuung vor Ort



20+
Standorte weltweit mit Cyber-Ressourcen

100+
Cyber-Versicherungsspezialisten

400+
globale Großkunden



Software-Tools für mehr Cyber-Sicherheit
Cyber-Risiken analytisch erfassen

Willis Towers Watson bietet Ihnen selbst entwickelte Software-Tools, um Ihre Cyber-Risiken analytisch zu erfassen und maßgeschneiderte Lösungen zu gestalten.

In unsere Tools haben wir unsere Expertise aus den Bereichen HR-Management, Risikomanagement und Broking einfließen lassen. Diese Expertise steht Ihnen für vielfältige Diagnosen, Szenario-Analysen und Modellierungen „auf Knopfdruck“ zur Verfügung – eine Auswahl:

Cyber Risk Culture Survey

Mit unserem Tool „Cyber Risk Culture Survey“ können Unternehmen ihre Cyber-Sicherheits-Kultur bewerten, indem sie entsprechende Einstellungen und Verhaltensweisen ihrer Mitarbeiter transparent machen. Der Fokus liegt darauf, Schwachstellen zu identifizieren und ein Bewusstsein zu schaffen, das die Mitarbeiter Cyber-sicher handeln lässt.

Cyber Work Readiness Diagnostic

Unser Tool „Cyber Work Readiness Diagnostic“ hilft Unternehmen, eine Workforce-Strategie mit Blick auf „Cyber-Work“ zu entwickeln, sicherheitsrelevante Talent- und Skill-Lücken zu identifizieren und einen Recruiting- und Retention-Plan zu etablieren, der ihren Erfolg im Wettbewerb um Cyber-Talente sichert.

Cyber Quantified und Cyber Risk Profile Diagnostic

Mit Hilfe unserer Tools „Cyber Quantified“ und „Cyber Risk Profile Diagnostic“ können Unternehmen strategisch klar entscheiden, in welche prioritären Bereiche sie ihre Mittel am wirkungsvollsten investieren. Dazu gehören auch Investitionsentscheidungen mit Blick auf den Transfer finanzieller Risiken.

Dialog
Miteinander ins Gespräch kommen

Sie haben viele Möglichkeiten, die Cyber-Sicherheit Ihres Unternehmens mit uns zu steigern. Wenn wir mit Ihnen darüber reden dürfen, freuen wir uns!

Ihre Ansprechpartner

Möchten Sie mehr über unsere Expertise und Erfahrung oder über unsere Ansätze und IT-Tools erfahren? Dann können Sie sich gerne direkt an folgende Ansprechpartner wenden:

Marcus Kuhn, LL.M.
Manager Finex

marcus.kuhn@willistowerswatson.com
+49 69 848455-1225
+49 175 4431872

Thomas Purann
Lead Consultant Cyber Risk Solution DACH

thomas.purann@willistowerswatson.com
+49 89 840382-3120
+49 151 2614 7574

Gerald Sonnleitner
Head of Technology, Media, Telecommunication

gerald.sonnleitner@willistowerswatson.com
+49 221 17917-2605
+49 170 8096746

Über Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) gehört zu den weltweit führenden Unternehmen in den Bereichen Advisory, Broking und Solutions. Wir unterstützen unsere Kunden dabei, aus Risiken nachhaltiges Wachstum zu generieren. Unsere Wurzeln reichen bis in das Jahr 1828 zurück – heute ist Willis Towers Watson mit 45.000 Mitarbeitern in über 140 Ländern und Märkten aktiv. Wir gestalten und liefern Lösungen, die Risiken beherrschbar machen, Investitionen in die Mitarbeiter optimieren, Talente fördern und die Kapitalkraft steigern. So schützen und stärken wir Unternehmen und Mitarbeiter. Unsere einzigartige Perspektive bietet uns einen Blick auf die erfolgskritische Verbindung personalwirtschaftlicher Chancen, finanzwirtschaftlicher Möglichkeiten und innovativem Wissen – die dynamische Formel, um die Unternehmensperformance zu steigern. Gemeinsam machen wir Potenziale produktiv. Mehr Informationen finden Sie unter willistowerswatson.de

WTW-WE-D-0026 April 2019

willistowerswatson.de

Willis Towers Watson