www.pwc.de

Ein sicherer Deal?

Wie sich Private-Equity-Unternehmen gegen Cyberrisiken wappnen und ihr Beteiligungsportfolio vor Wertverlusten schützen können.

pwc

Inhaltsverzeichnis

A Einleitung ... 3

B Lagebild – Bedrohungsfaktor Cyberkriminalität ... 5

C Der regulatorische Handlungsdruck nimmt zu ... 8

D Cyberrisiken im Beteiligungsportfolio managen ... 12

E Sicherheitslücken als Deal Breaker – Ziele richtig bewerten ... 15

F Vier Schritte zum (cyber-)sicheren Deal ... 20

G Wie wir Sie unterstützen können ... 23

Ihre Ansprechpersonen ... 25

A Einleitung

Cybervorfälle können die Unternehmenswerte auf einen Schlag drastisch mindern. Dennoch verfügen viele Firmen über keine angemessene Sicherheitsausstattung. Für Private-Equity(PE)-Gesellschaften ergibt sich hieraus ein brisanter Risikococktail: Einerseits drohen ihnen signifikante Wertminderungen infolge von Cyberattacken durch hochprofessionell agierende und bestens organisierte Cyberkriminelle – sowohl in der Halteperiode von Portfoliounternehmen als auch während des Transaktionsprozesses. Andererseits sind die regulatorischen Anforderungen an eine angemessene Cybersicherheit massiv gestiegen. Verstöße ziehen hohe Strafzahlungen sowie Haftungsrisiken für die verantwortlichen Führungskräfte nach sich. Wie lässt sich dieses Risiko minimieren und zugleich der Wert des Beteiligungsportfolios schützen oder durch mehr Cybersicherheit sogar erhöhen? Wir beleuchten die Gefahrenlage, analysieren die größten Bedrohungen für PE-Investoren und zeigen, wie diese sich angemessen absichern können.

B Lagebild – Bedrohungsfaktor Cyberkriminalität

Florierende Cyberkriminalität bedroht Unternehmen jeglicher Größe

Wer die jüngste Entwicklung der Bedrohungslage durch Cyberangriffe verfolgt hat, musste zahlreiche Hiobsbotschaften verkraften. Seit Jahren gilt die Situation als sehr angespannt – und sie spitzt sich weiter zu. In Deutschland ist die Zahl der Cyberangriffe 2022 im Vergleich zum Vorjahr um 30 Prozent gestiegen. Laut den *Cyberattack Statistics 2023* von Check Point Research meldeten Organisationen im ersten Quartal 2023 pro Woche durchschnittlich jeweils knapp 900 Angriffe. Der jährliche Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) verzeichnete 2022 eine Zunahme der Malware-Varianten um 116 Millionen im Vergleich zum Berichtszeitraum davor. Auch die Zahl der in Deutschland bekannt gewordenen Schwachstellen ist im vergangenen Jahr gestiegen. Der Gesamtschaden für die deutsche Wirtschaft durch Cyberangriffe, Sabotage und IT-Diebstahl lag laut Bitkom 2022 bei rund 203 Milliarden Euro.

Eine Entspannung ist nicht in Sicht, im Gegenteil. Für Cyberkriminelle war es noch nie so leicht, hochprofessionelle Angriffe gegen Unternehmen zu fahren. Sie schöpfen aus einem reichen Arsenal an Werkzeugen und Unterstützungsangeboten – von How-to-Hack-Tutorials über Deepfake-Software bis hin zu KI-Systemen wie ChatGPT, mit denen sich in Sekundenschnelle glaubwürdige und maßgeschneiderte Phishing-Mails generieren lassen. Wer heute ein Unternehmen um Millionenbeträge erleichtern will, braucht keine außergewöhnlichen Hacking-Fähigkeiten. Alle Zutaten für einen erfolgreichen Angriff lassen sich bequem aus dem Darknet – einem anonymen, vom Internet isolierten Netzwerk – beziehen. Die florierende Untergrundökonomie ist bestens organisiert und hat für fast jeden Fall ein passendes „Hacking-as-a-Service“-Angebot parat.

Im Fadenkreuz der Hacker stehen Unternehmen jeder Größe. Wer glaubt, seine Firma sei zu klein oder zu uninteressant, irrt gewaltig. Die Cyberkriminellen wissen genau, dass viele kleine und mittlere Unternehmen nicht über eine angemessene Sicherheitsausstattung verfügen. Gerade kleinere Unternehmen investieren vorrangig in die Entwicklung neuer Produkte sowie Services und vernachlässigen die Ausgaben für IT-Sicherheit – zumindest so lange, bis sie den ersten Cybervorfall und den daraus resultierenden Schaden zu spüren bekommen.

Die PE-Branche bietet attraktive Angriffsziele

Sowohl PE-Gesellschaften als auch deren Portfoliounternehmen sind beliebte Ziele von Cyberkriminellen. Ein Grund dafür ist deren oft unzureichende Sicherheitsinfrastruktur. Zwar ist das Bewusstsein für Cyberrisiken bei den PE-Gesellschaften in den letzten Jahren gewachsen. Bei der praktischen Umsetzung adäquater Schutzmaßnahmen gibt es jedoch noch viel Luft nach oben. Nur wenige Unternehmen verfolgen konsequent einen ganzheitlichen Ansatz. Auch bei der Bewertung von Zielunternehmen agieren einige PE-Investoren fahrlässig, indem sie die Cyberrisiken in ihrem Portfolio nicht ausreichend unter die Lupe nehmen. Einer Studie von Blue Voyant zufolge ist jedes fünfte Portfoliounternehmen durch eine bereits bekannte kritische Sicherheitslücke gefährdet.

Ein weiterer Grund, weshalb die PE-Branche für Cyberkriminelle immer attraktiver wird, liegt in der Natur von Deals: Hier wechseln große Geldsummen den Besitzer und streng vertrauliche Daten werden ausgetauscht. Viele Akteur:innen wie Anwält:innen, Banker:innen und Berater:innen agieren unter hohem Zeitdruck. Daraus ergibt sich ein sehr fruchtbarer Boden für Betrügereien wie das Abgreifen sensibler Daten oder die Umleitung von Überweisungen durch Täuschung der Beteiligten (Social Engineering).

Während die Cyberkriminellen bestens organisiert sind und in allen nur erdenklichen Fällen sehr erfolgreich miteinander kooperieren, mangelt es in der Wirtschaft an Offenheit und Transparenz. Die wenigsten Unternehmen trauen sich, offen über einen Cybervorfall zu sprechen.

Cyber-Equity-Story: Sicherheit als Unternehmenswert

Trotz aller Gefahren durch potenzielle Cyberangriffe sollten insbesondere PE-Häuser das Thema Cybersicherheit nicht nur als einen ungeliebten Block an notwendigen Ausgaben zur Werterhaltung verstehen. Denn wie gut ein Unternehmen in Sachen Cybersicherheit aufgestellt ist, beeinflusst seinen Wert in zweifacher Hinsicht: Erfüllen Portfoliounternehmen nachweislich bestimmte Sicherheitsstandards und sind sie angemessen abgesichert, so steigt nicht nur ihre Resilienz gegen Angriffe aus dem Cyberraum, sondern auch ihr Unternehmenswert.

Wenn das IT-Sicherheitsniveau überzeugt, lassen sich schon heute beim Exit vier bis fünf Prozent höhere Verkaufspreise erzielen. In Zukunft könnten die erzielbaren Gewinne weiter steigen – zumal einige Cyberrisiken inzwischen kaum noch versicherbar sind. Für PE-Investoren bietet Cybersicherheit deshalb auch die Chance, den Wert ihrer Beteiligungen systematisch zu erhöhen und die Verbesserungen wirkungsvoll in einer Cyber-Equity-Story zu kommunizieren.

Key Takeaways

- Cyberkriminalität floriert, die Lage ist sehr angespannt. Die Angreifer:innen sind bestens organisiert und nehmen Unternehmen jeglicher Größe ins Visier.
- Kapitalbeteiligungsgesellschaften und ihre Beteiligungsunternehmen stellen lukrative Angriffsziele für Cyberkriminelle dar – gerade im Transaktionskontext. Die Schutzmaßnahmen vieler PE-Häuser und ihrer Beteiligungen sind unzureichend.
- Investitionen in die Cybersicherheit steigern den Wert eines Unternehmens. Mit einer entsprechenden Cyber-Equity-Story lassen sich höhere Verkaufspreise erzielen.

C Der regulatorische Handlungsdruck nimmt zu

Ausweitung gesetzlicher Vorgaben auf neue Branchen und Sektoren

Die stetig zunehmenden Gefahren durch Cyberattacken und die immer drastischeren Auswirkungen haben längst auch den Gesetzgeber auf den Plan gerufen. Vor 20 Jahren war die Zahl der Systeme, die nach einer Kompromittierung massiven Schaden anrichten konnten, noch überschaubar. Heute gibt es unzählige Szenarien, wie gehackte Systeme nicht nur die Wirtschaftskraft beeinträchtigen, sondern auch Menschenleben gefährden oder zu großflächigen Gefahrenlagen führen – vom gehackten vernetzten Herzschrittmacher oder Fahrassistenzsystem bis hin zum Blackout durch Angriffe auf die Energieversorgung. Folgerichtig werden auch die gesetzlichen Regelwerke an die neue Bedrohungslage angepasst.

In vielen Branchen gelten spezifische gesetzliche Vorgaben. Zusätzlich gibt es übergeordnete Regelwerke, die mehrere Sektoren betreffen. Erst kürzlich trat die Network-and-Information-Security(NIS)-2-Richtlinie in Kraft, die auf ein hohes gemeinsames Cybersicherheitsniveau innerhalb der EU zielt. Sie verpflichtet die Mitgliedstaaten zum einen beispielsweise eine nationale Cybersicherheitsstrategie zu verabschieden und Behörden für das Krisenmanagement von Cyberangriffen einzurichten. Zum anderen sieht sie neue Pflichten für Unternehmen vor, die in 18 Sektoren als Betreiber kritischer Infrastrukturen (KRITIS) eingestuft sind.

Für die deutsche KRITIS-Regulierung bringt NIS-2 einschneidende Änderungen. Deutlich mehr Unternehmen sind künftig betroffen und die zu erfüllenden Pflichten werden konkreter und detaillierter. Neue Vorgaben für das Risikomanagement in Hinblick auf Cybergefahren verpflichten die Unternehmen, bestimmte Sicherheitsanforderungen einzuhalten, technische Maßnahmen zu ergreifen und Governance-Strukturen einzuführen. Hinzu kommen weitere Berichtspflichten für die Meldung bestimmter Sicherheitsvorfälle, die auf eine höhere Transparenz über die Gefahrenlage abzielen.

NIS-2 – aktualisierte EU-Vorschrift für Cybersicherheit

Die NIS-2-Richtlinie (EU 2022/2555) schafft einen modernisierten Rechtsrahmen und aktualisiert die 2016 eingeführten EU-Vorschriften zur Cybersicherheit. Sie ist seit Anfang 2023 in Kraft und muss bis Oktober 2024 von den Mitgliedstaaten in nationales Recht überführt werden. In Deutschland gibt es bereits einen Referentenentwurf des Bundesinnenministeriums zur Umsetzung der Richtlinie (NIS2UmsuCG). Gegenüber den ursprünglichen Regeln wurde der Geltungsbereich deutlich erweitert. Neben elf Sektoren mit hoher Kritikalität – von Energie und Verkehr über Bankwesen und Finanzmarktinfrastrukturen bis hin zum Gesundheitswesen – sind sieben weitere kritische Sektoren benannt, unter anderem Produktion, Verarbeitung und Vertrieb von Lebensmitteln und die Herstellung bestimmter Waren. Unternehmen ab 50 Mitarbeiter:innen oder mit mehr als zehn Millionen Euro Umsatz, die als Betreiber in den genannten Sektoren eingestuft sind, müssen neuen Sicherheits- und Meldepflichten nachkommen. Bei Verstößen drohen Strafzahlungen von bis zu zwei Prozent des Jahresumsatzes.

Mehr Informationen dazu finden Sie auf www.pwc.de/NIS2.

Für PE-Unternehmen ist NIS-2 besonders relevant, da sich aus dieser Richtline für die Cybersicherheit zahlreicher Portfoliounternehmen potenziell neue Anforderungen und gesetzliche Pflichten ergeben. Ausgenommen von der Regelung sind lediglich kleine und kleinste Unternehmen, die eine Zahl von 49 Mitarbeiter:innen oder einen Umsatz von zehn Millionen Euro nicht überschreiten. Sind mehrere Portfoliounternehmen von der neuen Regelung betroffen, so sollten die PE-Investoren ausloten, welche Synergien sich für die NIS-2-Umsetzung anbieten und ob dabei benötigte Dienstleistungen zentral bezogen werden können.

Übersicht der in Anhang 1 und 2 der NIS-2-Richtlinie gelisteten Sektoren

wesentliche Sektoren	wichtige Sektoren
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarkt-infrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	verarbeitendes Gewerbe/ Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung
digitale Infrastruktur	
Verwaltung von IKT-Diensten (B2B)	
öffentliche Verwaltung	
Weltraum	

Risiken durch Datenschutzverstöße

Ein besonderes Gefahrenpotenzial stellen nicht ausreichend geschützte Daten dar. Hacker haben es bei ihren Angriffen vor allem auf die Kund:innendaten der Unternehmen abgesehen. Dazu gehören sensible Informationen wie Namen, Geburtsdaten, Adressen, Bankverbindungen und Sozialversicherungsnummern. Mit den eingesehenen oder entwendeten Daten erpressen sie beispielsweise Lösegelder, indem sie mit der Veröffentlichung drohen. Darüber hinaus sind solche Datensätze beliebte Güter auf den Marktplätzen im Darknet.

Der Verlust von personenbezogenen Daten bedroht je nach Situation nicht nur das Geschäft und die Reputation eines Unternehmens. Er ist auch ein folgenschwerer Verstoß gegen die 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO). Für die kommenden Jahre ist zu erwarten, dass die Aufsichtsbehörden die Durchsetzung der Datenschutzgesetze weiter verstärken werden.

Welche Sanktionen bei Verstößen drohen

Die gesetzlichen Regelungen rund um Cybersicherheit und Datenschutz sind nicht zu unterschätzen. In den vergangenen Jahren wurden Verstöße immer systematischer geahndet und Strafzahlungen stiegen. So beschloss der Europäische Datenschutzausschuss am 12. Mai 2022 ein neues Bußgeldmodell für Verstöße gegen die DSGVO. Der gesetzliche Höchstrahmen für Bußgelder kann seitdem bis zu 20 Millionen Euro bzw. vier Prozent des Vorjahresumsatzes betragen. Im Jahr 2022 verhängten die europäischen Datenschutzbehörden Bußgelder in Höhe von fast drei Milliarden Euro. Die höchsten Strafen trafen dabei große Technologiefirmen wie Amazon und Meta.

Mit dem IT-Sicherheitsgesetz 2.0 von 2021 erhöhten sich auch die Bußgelder bei Verstößen gegen die KRITIS-Regulierung. Ferner sind neue Tatbestände hinzugekommen. Die Zuwiderhandlung gegen eine Anordnung des BSI zur Behebung eines Sicherheitsmangels kann mit bis zu 20 Millionen Euro geahndet werden. Wird ein Störfall nicht gemeldet, so kann eine Strafzahlung von 500.000 Euro fällig werden. Mit Umsetzung der NIS-2-Richtlinie in nationales Recht drohen weitere Geldbußen. Wer als Unternehmen gegen Artikel 21 (Risikomaßnahmen im Bereich der Cybersicherheit) oder 23 (Berichtspflichten) verstößt, riskiert Strafen von bis zu zehn Millionen Euro oder zwei Prozent des Umsatzes.

Da bei einem Cybervorfall sehr schnell Verstöße gegen verpflichtende Sicherheitsmaßnahmen sowie Datenschutzverstöße gleichzeitig auftreten können, liegen möglicherweise mehrere Tatbestände auf einmal vor. Dadurch sind in Ausnahmefällen Strafzahlungen von bis zu sechs Prozent des Umsatzes möglich. Für die Umsetzung der Sicherheitsmaßnahmen in ihrer Einrichtung haftet die Geschäftsführung auch persönlich. So legt Artikel 32 Abs. 6 der NIS-2-Richtlinie ausdrücklich die Verantwortlichkeit und Haftung von natürlichen Personen fest, die für wesentliche Einrichtungen verantwortlich sind.

Key Takeaways

- Die gesetzlichen Anforderungen für Unternehmen an die Cybersicherheit steigen. Mit der NIS-2-Richtlinie ergeben sich in 18 Sektoren neue Pflichten für das Management von Cyberrisiken.
- Cyberkriminelle haben es bei Angriffen häufig auf Kund:innendaten abgesehen. Eine hohe Datensicherheit ist unabdingbar, um die Vorgaben der DSGVO einzuhalten.
- Verstöße gegen Cybersicherheitsvorgaben werden systematischer und mit höheren Bußgeldern geahndet. Schlimmstenfalls drohen Strafzahlungen von bis zu sechs Prozent des Umsatzes.

D Cyberrisiken im Beteiligungs-portfolio managen

Wie die Portfoliostrategie mit Cyberrisiken zusammenhängt

Welchen Cyberrisiken PE-Unternehmen ausgesetzt sind, richtet sich maßgeblich nach ihrer Portfoliostrategie. Einen wesentlichen Anhaltspunkt liefert der Branchenschwer punkt. Wer sich beispielsweise auf Beteiligungen im Energiesektor oder im Gesundheitswesen spezialisiert hat, muss allein infolge der KRITIS-Verordnung und der NIS-2-Richtlinie die Einhaltung hoher Sicherheitsanforderungen sicherstellen und ist in jedem Fall mit hohen regulatorischen Risiken konfrontiert.

Auch die Anzahl und Vielfalt der Beteiligungen und die damit verbundenen Risiko-Rendite-Profile wirken sich auf das Ausmaß der Cyberrisiken aus: Ein großes Portfolio bietet eine größere Angriffsfläche. Ein kleines Portfolio führt zu einem höheren Konzentrationsrisiko. Wenn einzelne Beteiligungen einen großen Anteil am Gesamtwert ausmachen, dann haben Cybervorfälle an diesen Stellen weitaus gravierendere Auswirkungen.

Um nicht von den katastrophalen Folgen eines Cybervorfalls überrascht zu werden, müssen PE-Investoren ein Bewusstsein für die Schwachstellen und Risiken in ihrem Portfolio entwickeln und die richtigen Sicherheitsmaßnahmen ergreifen. Der Schlüssel dazu ist ein übergreifendes Cyberrisikomanagement.

Kontinuierliches Monitoring von Schwachstellen und Bedrohungen

Cyberkriminelle entwickeln ihre Methoden und Angriffstechniken ständig weiter. Jeden Tag entstehen hunderttausende neue Malware-Varianten. Bekannt gewordene Schwachstellen werden immer schneller im großen Stil ausgenutzt. Das einmalige Überprüfen des Portfolios auf Schwachstellen und Bedrohungen ist deshalb nur für eine sehr kurze Zeitspanne aussagekräftig. Wer sein Portfolio dauerhafter vor Wertverlusten schützen möchte, benötigt ein Cyberrisikomanagement, das auf kontinuierliches Monitoring setzt.

Um herauszufinden, welche Schwachstellen einzelne Beteiligungen aufweisen und welchen Bedrohungen sie ausgesetzt sind, gibt es effektive Methoden und Services von spezialisierten Dienstleistern. Der Umfang und Detailgrad der Analysen – sogenannte PortCo-Cyberscans – lässt sich dabei individuell anpassen, zum Beispiel an den Umfang der Anteile an Beteiligungen sowie verschiedene Risikoprofile.

Bedrohungen proaktiv begegnen

Die Auswertungen der regelmäßigen PortCo-Cyberscans fassen kritische Funde zusammen und geben Handlungsempfehlungen für eine angemessene Absicherung. Die Berichte enthalten zum Beispiel eine Liste gefährdeter Dienste, identifizierter Malware-Infektionen, geleakter E-Mail-Anmeldedaten sowie Typo-Squatting-Domains, die bei Tippfehlern in der URL von Diensten unter anderem zum Abgreifen von Accountdaten genutzt werden.

Ein Beispiel aus der Praxis von PwC: In einem unserer letzten Projekte haben wir für unseren Kunden 30 Portfoliounternehmen gescannt. Dabei wurden über 70 Bedrohungen identifiziert, von denen 25 als kritisch eingestuft wurden und sofort behoben werden mussten. Weitere 20 Bedrohungen stellten weniger zeitkritische, aber nicht minder gefährliche Schwachstellen dar und mussten kurzfristig angegangen werden.

Die während der Scans identifizierten Befunde bestanden zum einen aus häufig beobachteten Schwachstellen wie veralteten JavaScript-Bibliotheken und abgelaufenen digitalen Zertifikaten. Zum anderen wurden aber auch Schwachstellen in kritischen Anwendungen aufgedeckt, die – wenn sie ausgenutzt werden – zu Datenschutzverletzungen, Unterbrechungen des Geschäftsbetriebs und dem Verlust von geistigem Eigentum führen können.

Grundsätzlich ist zu berücksichtigen, dass ein Scan nur den Zustand zu einem bestimmten Zeitpunkt untersucht. Die Cyberbedrohungen entwickeln sich aber ständig weiter. Oft vergehen zwischen der Entdeckung einer Schwachstelle und ihrer Ausnutzung nur wenige Tage. Mit den Berichten der Cyberscans erhalten PE-Investoren nicht nur ein klares Bild über die Bedrohungslage innerhalb ihres Beteiligungsportfolios. Sie verfügen damit auch über die Entscheidungsgrundlage für eine proaktive Planung und Umsetzung von Schutzmaßnahmen. Wenn in mehreren Portfoliounternehmen ähnliche Maßnahmen anstehen, dann lassen sich durch die Bündelung des Auftrags bei einem Dienstleister unter Umständen Preisvorteile erzielen.

Key Takeaways

- Die Umsetzung von Sicherheitsmaßnahmen sollte auf die Portfoliostrategie abgestimmt sein und die spezifischen Cyberrisiken angemessen berücksichtigen.
- Aufgrund der dynamischen Bedrohungslage ist ein kontinuierliches Monitoring der Schwachstellen von Beteiligungen unabdingbar, um die Cyberrisiken des Portfolios zu bewerten.
- PortCo-Cyberscans liefern Daten für eine fundierte Risikobewertung und ermöglichen so die systematische Planung und Umsetzung von Schutzmaßnahmen.

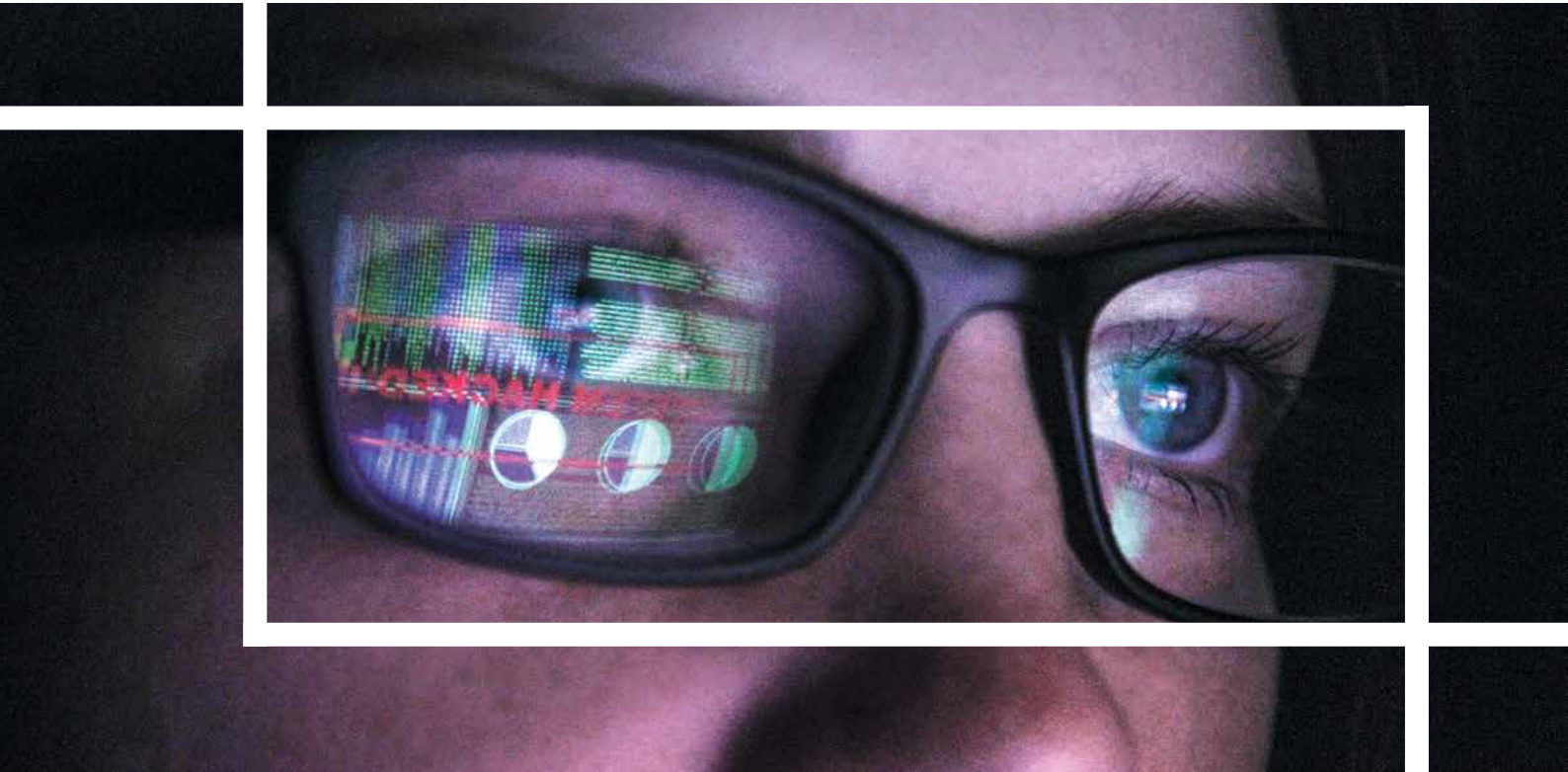
E Sicherheitslücken als Deal Breaker – Ziele richtig bewerten

Cyberrisiken erkennen – alles andere als überbewertet
Obwohl die Resilienz gegenüber Cyberrisiken den Unternehmenswert deutlich verbessert, wird sie noch nicht von allen PE-Gesellschaften systematisch für die Bewertung von Zielen herangezogen. In der Praxis haben wir zahlreiche Fälle erlebt, in denen die durchgeführten Schwachstellenscans und Cyber Security-Due-Diligences eine erschreckende Anfälligkeit für Cybervorfälle offenbarten. Wer an einem Assessment „spart“, kauft die Katze im Sack und erwirbt ein Unternehmen möglicherweise weit über Wert.

Neben dem Risiko der Überbewertung drohen immense Folgekosten bei einem Cybervorfall. Eine erfolgreiche Ransomware-Attacke mit zusätzlich entwendeten Kund:innendaten reicht aus, um den Unternehmenswert regelrecht verpuffen zu lassen. Wird bekannt, dass die Sicherheitsvorkehrungen unzureichend waren, drohen massive Reputationsverluste und eventuell auch Haftungsansprüche gegen das Management.

Cyber Security Due Diligence ist Pflicht
Im digitalen Zeitalter können unzureichende Vorkehrungen zur Cybersicherheit ein Deal Breaker sein. Dem Käufer drohen nach der Übernahme unerwartete Kosten für die Behebung kritischer Sicherheitslücken. Um Risiken zu identifizieren und Abweichungen des Wertes zu erkennen, sollten die PE-Unternehmen vor jedem Deal eine Cyber Security Due Diligence durchführen. Die dabei aufgedeckten Sicherheitsrisiken können dann in den Verhandlungen diskutiert werden. Sie liefern zudem eine wichtige Basis für weitere Schritte, etwa die Behebung von Schwachstellen.

Für einen ganzheitlichen Überblick wird das Zielunternehmen dabei üblicherweise in verschiedenen Dimensionen beleuchtet. Abbildung 1 zeigt beispielhaft die Prüfungsdimensionen, die PwC bei einer Cyber Security Due Diligence zugrunde legt.



Dimensionen der Cyber Security Due Diligence (Ausschnitt)

	Red Flag	Extended (ergänzend zu Red Flag)
organisatorisch	• Analyse der Cybersicherheitsstrategie • Bewertung der Cybersicherheits-Governance • Überprüfung der IT-Sicherheitsorganisation	• Bewertung von Prozessen im Zusammenhang mit Cybersicherheit • Analyse der Rollen im Bereich der Cybersicherheit
technologisch	• Bewertung des Schwachstellenmanagements • Analyse der Erkennungs- und Reaktionsmechanismen • Check der Backup- und Recovery-Prozesse	• Überprüfung der Verfahren für sichere Softwareentwicklung entlang des Lebenszyklus • Analyse der eingesetzten Cybersicherheits tools
personenbezogen	• Review der Kurse und Lernmaßnahmen zu Informationssicherheit für die Mitarbeitenden • Analyse des Sicherheitsbewusstseins und der Sicherheitskultur	• Überprüfung der gesicherten Umgebung für Remote Work • Evaluierung von KPIs für Maßnahmen zum Sicherheitsbewusstsein
physisch	• Analyse des Perimeterschutzes • Begutachtung der Zugangskontrollen und Zutrittsbeschränkungen	• Inspektion der unterstützenden Hilfsmittel • Überprüfung von „Clear Desk“- und „Clear Screen“-Maßnahmen
externe Quellen	• Recherchen im Netz zu relevanten aktuellen Schwachstellen und Bedrohungen	• Recherche in spezialisierten Sicherheitsforen über die Exponiertheit des Unternehmens hinsichtlich Informationslecks, Schwachstellen, Sicherheitsverletzungen

Fallstudie

Die Situation

Ein deutsches Technologieunternehmen plante den Einstieg in den Markt für Metaverse und VR-Gadgets. Um sich die notwendigen Fähigkeiten anzueignen und den Markteintritt zu beschleunigen, wollte es ein führendes Metaverse-Start-up übernehmen. Vor zwei Jahren kam es bei dem Start-up zu einem Sicherheitsverstoß, bei dem Hacker unrechtmäßig an zwei Millionen Datensätze gelangten, darunter persönliche Daten wie Geburtsdaten, Namen und Sicherheitsinformationen. Das Start-up führte nach eigenen Angaben eine Untersuchung durch und gab eine öffentliche Erklärung ab, in der der Vorfall einem Mitarbeiter eines Zulieferers zugeschrieben wurde, der Opfer eines Phishing-Angriffs geworden war.

Dennoch hielt das Technologieunternehmen aufgrund des erwarteten Potenzials an seinen Plänen fest, das Start-up zu akquirieren. PwC wurde beauftragt, eine Bewertung der Cyber Security-Organisation des Übernahmeziels durchzuführen.

Unser Ansatz

Im Rahmen der Cyber Security Due Diligence wurden die grundlegenden Richtlinien, Konzepte und Dokumentationen zur IT-Sicherheit und Informationssicherheit umfassend überprüft. Darüber hinaus besichtigten unsere Berater:innen den Standort und führten Interviews, um sich ein genaues Bild von der Sicherheitslage inklusive der physischen Sicherheitsmechanismen des Unternehmens zu machen.

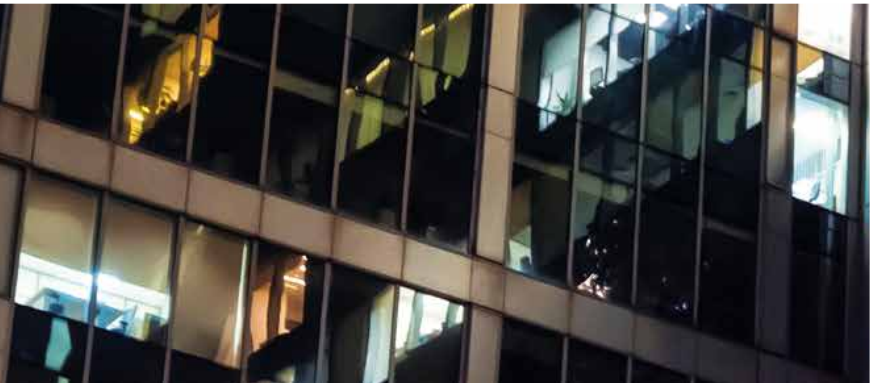
Das Projektergebnis

Die Analyse deckte kritische Schwachstellen in der IT-Infrastruktur und Sicherheitsarchitektur des Start-ups auf, die eine erhebliche Gefahr darstellten. Zwei E-Mail-Adressen von Mitarbeiter:innen waren geleakt worden. Der Schutz vor Cyberangriffen war unzureichend und wichtige Maßnahmen zur Absicherung der Vermögenswerte des Unternehmens waren nicht erkennbar. Die Verantwortlichkeiten im Bereich Datenschutz und Informationssicherheit waren nicht ausreichend definiert. Darüber hinaus wurden erhebliche Mängel bei den Incident-Response-Fähigkeiten festgestellt.

Unsere Expert:innen präsentierten die identifizierten Risiken in einem detaillierten Ergebnisbericht. Sie zeigten dem interessierten Käufer mögliche Kosten und Zeitaufwände auf, die mit den erforderlichen Sicherheitsmaßnahmen verbunden waren. Zudem wurden Empfehlungen für die Kaufpreisverhandlung ausgesprochen.

Key Takeaways

- Ohne die Berücksichtigung der Cyberresilienz eines Unternehmens vor dem Kauf droht die Gefahr der Überbewertung.
- Eine Cyber Security Due Diligence macht Cyberrisiken transparent. Sie verhindert nachträgliche Kosten für das Beheben von Sicherheitslücken.
- Die Ergebnisse einer Cyber Security Due Diligence sollten in die Verhandlungen mit eingebracht werden. Zudem tragen sie bei nachfolgenden Schritten zu mehr Cybersicherheit bei.



F Vier Schritte zum (cyber-)sicheren Deal

Handlungsempfehlungen

Cybersicherheit bewahrt PE-Investoren nicht nur vor den Betrugsversuchen professionell agierender Cyberkrimineller, sondern verschafft ihnen auch Wettbewerbsvorteile. Sie stärkt das Vertrauen von Kunden, Partnern und weiteren Stakeholdern, stellt die Einhaltung regulatorischer Anforderungen sicher und steigert Unternehmenswerte.

1. Regulatorische Vorgaben in Hinblick auf NIS-2 prüfen

Um die Einhaltung gesetzlicher Vorgaben im Bereich der Cybersicherheit zu gewährleisten, sollten PE-Investoren ein spezielles Cyberrisikomanagement einrichten. Dabei ist zunächst zu prüfen, welche regulatorischen Anforderungen überhaupt relevant sind. Durch die NIS-2-Richtlinie könnten auch Portfoliounternehmen, die bislang nicht als Betreiber kritischer Infrastrukturen eingestuft waren, mit strengeren Auflagen konfrontiert werden. Bei identifizierten Lücken sind entsprechende Maßnahmen zu planen und umzusetzen, um Bußgeldern vorzubeugen.

2. Mit PortCo-Scans das Portfolio schützen

Die kontinuierliche Analyse der Beteiligungen auf Schwachstellen und Bedrohungen schafft einerseits Transparenz darüber, wie stark eine Beteiligung, ein Beteiligungsportfolio, ein PE-Fonds bzw. das ganze PE-Haus zum Zeitpunkt der Scans exponiert ist. Andererseits bieten die dadurch erstellten Berichte eine fundierte Entscheidungsgrundlage für die gezielte Planung und Umsetzung von Schutzmaßnahmen. Die Portfoliostrategie und -struktur, kombiniert mit der individuellen Risikobereitschaft, sollten den Ausschlag darüber geben, welche Beteiligungen Portfolien und Fonds in welchem Umfang regelmäßig gescannt werden.

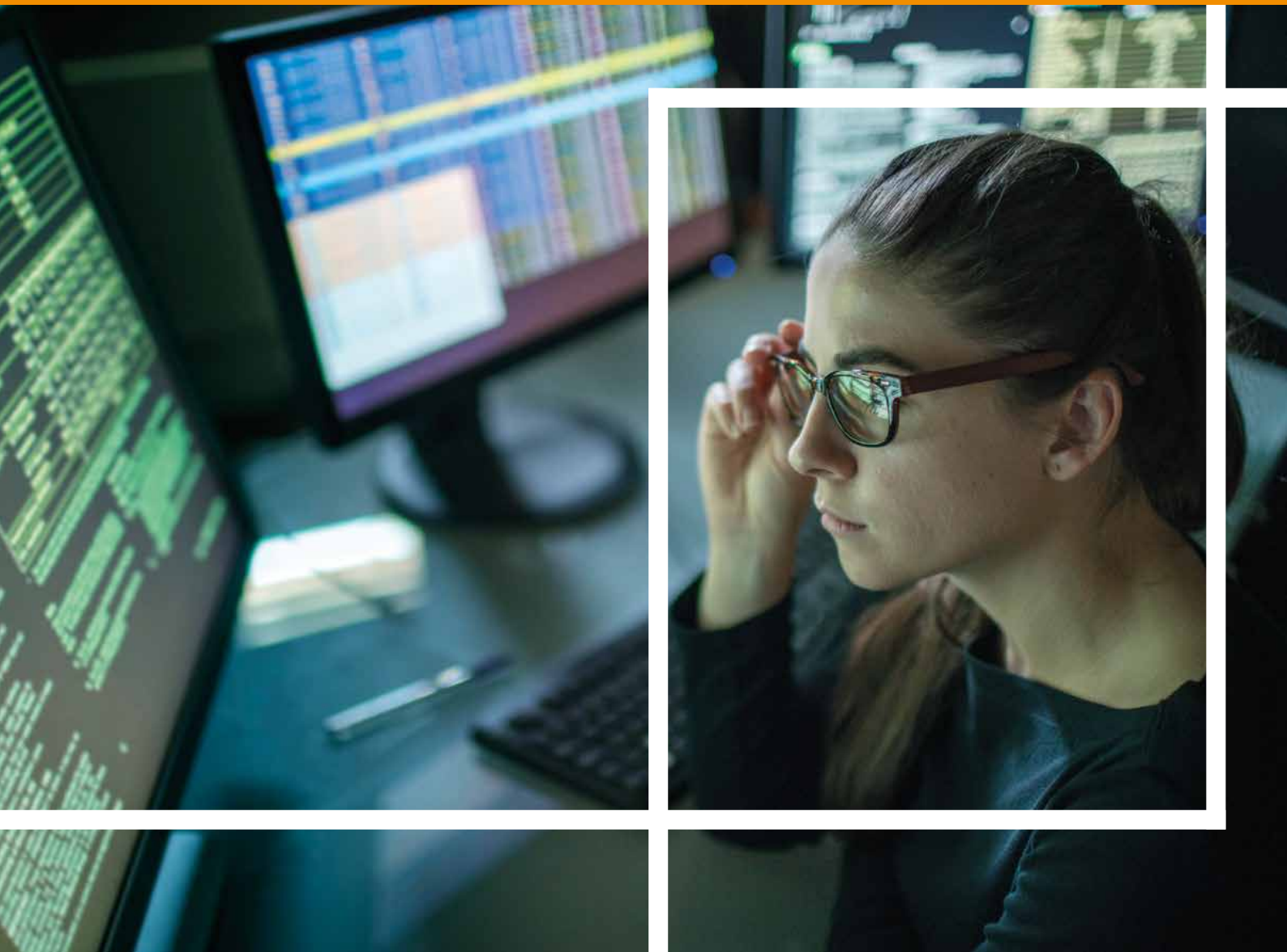
3. Vor jedem Kauf eine Cyber Security Due Diligence durchführen

Wer ein Unternehmen erwirbt, ohne vorab dessen Cyberresilienz zu prüfen, lässt sich womöglich übervorteilen. So besteht nicht nur die Gefahr der Überbewertung aufgrund von in der Vergangenheit vernachlässigten Investitionen in die Cybersicherheit. Viele Unternehmen sind zudem längst unbemerkt das Opfer eines Cyberangriffs geworden. So vergehen im Schnitt mehr als 240 Tage, bis ein Fall von gestohlenen oder kompromittierten Zugangsdaten erkannt wird, wie die Data Breach Studie 2022 von IBM errechnet hat. Bei einem Vorfall drohen massive Folgekosten und Reputationsschäden.

4. Cybersicherheit als Werttreiber nutzen

Eine verbesserte Sicherheitsausstattung im Unternehmen senkt das Risiko von Cyberangriffen und rechtfertigt eine höhere Bewertung. PE-Investoren können sich diesen Umstand zunutze machen und Investitionen in die Cybersicherheit in ihre Equity-Story einfließen lassen. Die regelmäßige Durchführung umfassender Cyberscans, der Aufbau einer sicheren IT-Infrastruktur und die Umsetzung weiterer Schutzmaßnahmen wie Awareness-Trainings führen zu einer Steigerung des Unternehmenswertes der Beteiligung während der Haltedauer und bis hin zum Exit. In der Praxis sind uns bereits Fälle begegnet, in denen eine nachgewiesene hohe Cyberresilienz zu Preissteigerungen von vier bis fünf Prozent geführt hat.

G Wie wir Sie unterstützen können



Unser engagiertes Team hilft Ihnen dabei, den Wert in jeder Phase des Deal-Lebenszyklus zu maximieren. Wir vereinen unser strategisches und technisches Know-how, um Cybersicherheitsrisiken, aber auch Chancen im Rahmen Ihres Deals aufzuzeigen. Dazu können wir auf unser globales PwC-Netzwerk aus Expert:innen für Cybersicherheit und für Transaktionen zugreifen. Mit unserer auf Ihre Anforderungen zugeschnittenen Beratung stehen wir Ihnen bei Ihren Investitionsentscheidungen, praktischen Aktionsplänen sowie Integrations- und Veräußerungsvorhaben zur Seite.

Cyber Security Framework für Deal-Advisory

Phase	Strategie und Planung	Due Diligence Cyber Security (DD)	Onboarding und Integration	Operations und Management	Divestiture und Exit
Ziele	Bewertungen von Insights und Unique Selling Point zur Unterstützung Ihrer Deals-Strategie	Bewertung der Cyber Resilience, Aufdecken versteckter Kosten durch Sicherheitslücken	umfassende Planung der Onboarding-Prozesse und Vorbereitung einer sicheren Integration	kontinuierliche Überwachung von Cyberbedrohungen und -schwachstellen, um Risiken zu mindern	angemessene Analysen und Vorbereitungen, um die Geschäftsabläufe sicherzustellen sowie Systemausfälle oder Datenverluste zu vermeiden
Instrumente	• Strategic Cyber Evaluation • Pre-deal Intelligence Mining	• Red Flag Cyber Security DD • Extended Cyber Security DD	• Cybersecurity Day 1 Assessment • Cybersecurity Integration Support	• Portfolio Company Scanning • M&A Security Framework	• Divestiture Security Check • Separation Security Services

Cybersecurity Framework für Deals

Ihre Ansprechpersonen

Private Equity

Steve Roberts
PwC Deutschland
Mobiltel.: +49 171 5572585
steven.m.roberts@pwc.com

Cyber Security & Privacy

Jörg Asma
PwC Deutschland
Mobiltel.: +49 160 6142945
joerg.asma@pwc.com

Andrea Schmitt
PwC Deutschland
Mobiltel.: +49 160 2742831
andrea.schmitt@pwc.com

Forensic Services

Arndt Engelmann
PwC Deutschland
Mobiltel.: +49 151 14806264
arndt.engelmann@pwc.com

Kira Kühl
PwC Deutschland
Mobiltel.: +49 151 67137691
kira.kuehl@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren 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 152 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. Mehr als 13.000 engagierte Menschen an 21 Standorten. Knapp 2,61 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

Die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft bekennt sich zu den PwCEthikgrundsätzen (zugänglich in deutscher Sprache über www.pwc.de/de/ethikcode) und zu den Zehn Prinzipien des UN Global Compact (zugänglich in deutscher und englischer Sprache über www.globalcompact.de).

© September 2023 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

www.pwc.de