PEak News@BDO

Cyber Security:

Unterschätzt Private Equity das Risiko?

März 2026

PEak News@BDO - Der Private Equity Newsletter für die DACH-Region

Cyber-Risiken immer noch unterschätzt

Cyber Security wird zunehmend zum kritischen Faktor für Portfolio-Unternehmen: Unzureichend geschützte Gesellschaften sind ein attraktives Ziel für Angriffe, was erhebliche finanzielle Schäden und Reputationsverluste nach sich ziehen kann und folglich Investitionsentscheidungen von Private-Equity-Investoren maßgeblich beeinflusst oder sogar gefährdet.

Aktuelle Zahlen der Bitkom Studie zum Wirtschaftsschutz (2025) beziffern den wirtschaftlichen Schaden durch Cyberangriffe auf jährlich rund 202,4 Milliarden Euro. Mit mehr als 70 % Anteil am Gesamtschaden für die deutsche Wirtschaft stehen Cybervorfälle damit an der Spitze der Bedrohungen für Unternehmen (Bitkom 2025, Allianz Risk Barometer 2025).

Die Zahl der Cyberangriffe ist auf einem globalen Allzeithoch, unbeeindruckt von Unternehmensgröße oder Branche. Untersuchungen zur Branchenzuordnung der Opfer von Cyberangriffen (IBM, 2024) verdeutlichen die übergreifende Relevanz von IT-bezogenen Risiken.

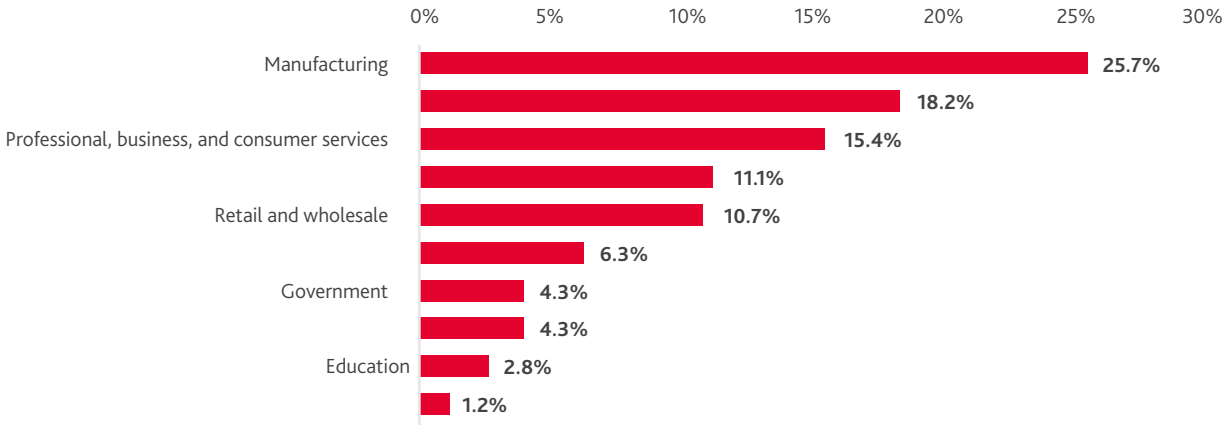

Abbildung 2 IBM: Branchenübersicht der Opfer von Cyberangriffen

Künstliche Intelligenz ist in aller Munde. Cyber-Kriminelle folgen diesem technologischen Trend: Die Nutzung von KI nimmt auch im Zusammenhang mit Cyberangriffen stetig zu, insbesondere in den Bereichen Phishing, Deepfakes und bei der Entwicklung neuartiger Malware. Gleichzeitig ist ein Rückgang der wahrgenommenen Resilienz deutscher Unternehmen zu beobachten: Nur noch jedes zweite Unternehmen fühlt sich auf Cyberangriffe sehr gut vorbereitet. Mehr als zwei Drittel der Unternehmen sehen durch Cyberangriffe ihre Existenz bedroht (Bitkom Wirtschaftsschutz 2025).

Doch Cyberrisiken sind längst kein reines IT-Thema mehr, sondern betreffen alle Ebenen eines Unternehmens – von der Führungsetage bis hin zur regulatorischen Compliance. Mit neuen EU-Regulierungen wie der DSGVO, NIS-2 und DORA wachsen die Anforderungen an Unternehmen deutlich. Verstöße gegen diese Vorschriften können empfindliche Bußgelder nach sich ziehen – ein erhebliches Risiko für Investoren, besonders in stark regulierten Branchen.

Auch als gezieltes Investment kann das Cyber Security-Segment interessant sein: Thoma Bravo investierte 2024 beispielsweise rund 5,3 Milliarden US-Dollar in die Übernahme des britischen Cyber Security-Anbieters Darktrace. In den DACH-Märkten stiegen Private-Equity-Häuser in den letzten fünf Jahren in über 20 Cyber Security-Unternehmen ein.

Für PE ist die Botschaft eindeutig: Cyber Security ist unverzichtbar geworden, um potenzielle Risiken frühzeitig zu erkennen und zu mitigieren. Wer Cyberrisiken unterschätzt oder zu spät adressiert, gefährdet nicht nur den aktuellen Deal, sondern langfristig auch den Wert und die Performance seines Portfolios.

Dealbreaker oder Werttreiber?

Angesichts steigender Bedrohungen und regulatorischer Anforderungen stellt sich überdies die Frage: Muss eine unzureichende Cyber Security einen Deal nicht zum Scheitern bringen? Oder bietet das Thema gar Potenzial, aktiv zur Wertsteigerung beizutragen?

Die Frage, ob Dealbreaker oder strategischer Faktor für Wertsteigerungen, hängt von verschiedenen Faktoren ab. Die Stellschrauben dafür, ob ein Cyber-Sicherheitsvorfall zum GAU wird, erstrecken sich über den gesamten Investment-Lebenszyklus hinweg, von der Due Diligence über den operativen Betrieb bis hin zum Exit.

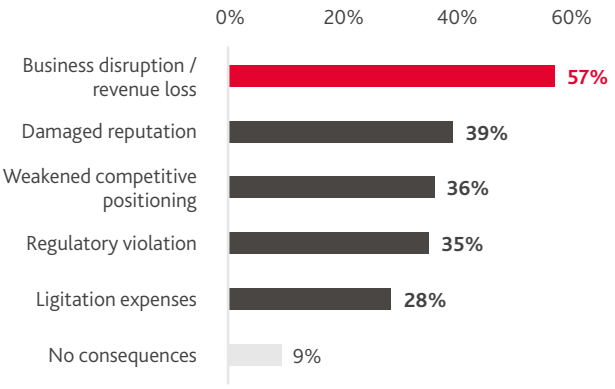

Abbildung 3 Proofpoint: Von betroffenen Unternehmen angegebene Konsequenzen von Cyberangriffen

Risikobetrachtung im Rahmen der Due Diligence

Die Due Diligence ist entscheidend dafür, Cyberrisiken frühzeitig aufzudecken und umfassend zu bewerten. Unternehmen mit Schwachstellen in ihrer IT-Infrastruktur riskieren nicht nur das Interesse potenzieller Investoren, sondern oftmals auch eine negative Anpassung des Kaufpreises. Grundlegende Analysefelder umfassen insbesondere:

- die Bewertung der bestehenden IT-Sicherheitsarchitektur,
- den Umgang mit sensiblen Daten sowie
- die Analyse und Aufarbeitung früherer Sicherheitsvorfälle.

Darüber hinaus sollte eine Due Diligence auch den Reifegrad der Sicherheitsmaßnahmen untersuchen, beispielsweise durch Zertifizierungen nach anerkannten Standards (wie z. B. ISO/IEC 27001 oder TISAX). Besonders wichtig ist zudem eine Prüfung der Lieferketten auf potenzielle Cyberrisiken, da Drittparteien oft Einfallstore für Angriffe darstellen. So gaben im Rahmen der Bitkom Wirtschaftsschutzstudie (2024) nur 37 % der befragten Unternehmen an, einen vollumfänglichen Plan zu besitzen, um auf Sicherheitsvorfälle in deren Lieferkette zu reagieren.

Personelle Faktoren wie die Existenz und Rolle eines Chief Information Security Officers (CISO) oder Informationssicherheitsbeauftragten (ISB) sowie klar definierte Verantwortlichkeiten auf Führungsebene sind ebenso kritisch zu evaluieren wie die Compliance mit regulatorischen Anforderungen. Zusätzlich sollte geprüft werden, ob ein ausreichender Versicherungsschutz die Auswirkungen von Cybervorfällen im Ernstfall minimieren kann.

Rolle der Investoren

Private-Equity-Investoren haben in Sachen Cyber Security zwei zentrale Rollen: Taktgeber und Werttreiber. Sie verankern Cyber-Risiken in Board-KPIs (z. B. Mean Time to Detect/Repair, (MTTD/MTTR) oder Patch Service Level Agreements), setzen klare Verantwortlichkeiten (z. B. CISO-Mandat oder Budgetierung) und verknüpfen Findings aus der Due Diligence mit Preis, Covenants und der Ausgestaltung von Transition Service Agreements. Der Wertbeitrag wirkt mit zweifachem Hebel: Downside-Absicherung (geringere Ausfallverluste, weniger Ausfälle, geringere Bußgelder, Cyber-Versicherungskosten) und Upside-Effekte (etwa Absatzsteigerungen durch Zertifizierung oder häufigere Lieferzulassungen in regulierten Branchen), was die Ergebnisse des Portfolio-Unternehmens stabilisiert und den Exit-Multiple stützen kann. Strategisch wird Cyber Security entlang der gesamten Wertschöpfungskette integriert: Bei Produktentwicklung (secure-by-design), robuster Daten-Governance, Third Party Risk Management und aller in jeder Lebenszyklusphase verwendeten Software (DevSecOps); die Due Diligence liefert die Roadmap, KPIs steuern die Umsetzung, und regelmäßige Reifegrad-Reviews halten die Cyber-Sicherheit des Portfolio-Unternehmens auf Kurs.

Cyber Security als Wertsteigerungsstrategie

Cyber Security hat sich längst von einer reinen Kostenposition zu einem strategischen Hebel für nachhaltige Wertsteigerung entwickelt. Unternehmen, die das Thema aktiv in ihrer Wachstumsstrategie verankern, profitieren auf mehreren Ebenen – nicht nur durch Risikoabsicherung, sondern vor allem durch deutlich verbesserte Marktchancen und erhöhten Unternehmenswert durch geringere Multiple-Abschläge.

How to Turn the Table: Der Weg zum resilienten Unternehmen

1. **Fokus auf die „Quick Wins“:**
   Konsequente Einführung von Multi-Faktor-Authentifizierung, grundlegendes Härten der zentralen Systeme, Zugriffsbeschränkungen durch sog. „Admin-Tiering“ sowie eine vollständige Asset- und Identity-Inventur bilden das Grundgerüst einer stabilen Infrastruktur.
2. **Nur wer erkennt, kann handeln:**
   Parallel dazu sollte durch die flächendeckende Einführung einer „Endpoint Detection & Response“ (EDR) Lösung in Verbindung mit einer zentralen Log-Aggregation eine Aufsicht auf die Systemlandschaft geschaffen werden. Nur mit einem solchen „Single Pane of Glass“ -Ansatz können Vorfälle effektiv erkannt und bearbeitet werden.
3. **Kein Backup, kein Mitleid:**
   Backups bilden die Rückversicherung im Ernstfall. Die Strategie sollte hier der „3-2-1 Regel“ folgen: Drei Datenkopien auf mindestens zwei verschiedenen Speichertypen, wovon eine Offsite verwahrt wird. So werden Totalausfälle des Systems vermieden und Ihre Daten sind im Notfall einsatzbereit, auch, wenn Teile des Systems betroffen sind. Und: Nur ein getestetes Backup ist ein echtes Backup!
4. **Ausbreitung verhindern:**
   Netzwerksegmentierung, Rechtevergabe nach dem Least-Privilege-Prinzip sowie die Einführung eines „Privileged Access Managements“ sind weitere Schritte in Richtung des Ziels, indem sie die Möglichkeiten der Ausbreitung im Ernstfall beschränken.
5. **Man kämpft nur so gut, wie man trainiert:**
   Regelmäßige Tests der Abläufe im Notfall in Form realistischer Tabletop-Exercises und Automatisierung von Reaktionsprozessen (z. B. durch Runbooks) verbessern die Abwehr.

Gesteuert über wenige Board-KPIs (z. B. Multifaktor-Authentifizierungs-Quote, kritische Patches < 14 Tage, Backup-Restore-Test), erzielen Portfolio-Unternehmen mit niedrigen CapEx (für Re-use/Konsolidierung) und planbaren OpEx (für SaaS) ein deutlich geringeres Cyber-Risiko, stabile EBITDA-Effekte – und einen robusteren Exit-Multiple.

Am wichtigsten ist jedoch eines: Anfangen! **Wer sich noch heute für Cyber Security entscheidet** und mit einem umfassenden **Cyber-Reifegrad-Assessment** startet, geht damit unmittelbar den ersten Schritt in Richtung einer nachhaltig etablierten Cyber Security.

Was früher ein reines Verteidigungsthema darstellte, hat sich mittlerweile zu einer aktiven Strategie zur Wertabsicherung und Differenzierung im Wettbewerb entwickelt. Unternehmen, die Cyber Security frühzeitig priorisieren, profitieren nachhaltig von höherem Vertrauen, gestärkten Kundenbeziehungen und besseren Investitionsmöglichkeiten. Für Private-Equity-Häuser eröffnet sich durch verbesserte Cyber Security zudem eine attraktive Chance auf die Realisierung der langfristigen Wertsteigerung ohne Abschläge bei Exit-Multiples.

Autoren:

Prof. Dr. Alexander Schinner

Partner
Incident Response, Business Continuity Management (BCM) &
Security Operation Center (SOC)
Tel.: +49 89 76906-167
alexander.schinner@bdosecurity.de

Jannik Schmied

Consultant
Incident Response
Tel.: +49 351 26352-184
jannik.schmied@bdosecurity.de

BDO AG Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12
20355 Hamburg
www.bdo.de

Private Equity-Ansprechpartner in der DACH-Region :

Dr. Michael Brauer
Tel.: +49 211 1371-186
michael.brauer@bdo.de

Dietmar Flügel
Tel.: +49 211 1371-162
dietmar.fluegel@bdo.de

Thorsten Schumacher
BDO Legal Rechtsanwaltsgesellschaft mbH
Tel.: +49 211 1371-323
thorsten.schumacher@bdolegal.de

Dr. Jan Faßhauer
Tel.: +49 69 95941-463
jan.fasshauer@bdo.de

Michael Maxeiner
Tel.: +49 211 1371-185
michael.maxeiner@bdo.de

Volkmar Berner
Tel.: +49 89 76906-458
volkmar.berner@bdo.de

Frank Scholl
Tel.: +49 40 30293-533
frank.scholl@bdo.de

Felix Fries
Tel.: +49 69 95941-195
felix.fries@bdo.de

BDO Österreich
Christoph Ernst
Tel.: +43 664 60 375-1643
christoph.ernst@bdo.at

BDO Schweiz
Benjamin Haldimann
Tel.: +41 44 444-3858
benjamin.haldimann@bdo.ch