Downloaded from PwC Blogs on 04.12.2025 10:40h

Insurance News Blog
By PwC Deutschland | 14. Januar 2025

Das Problem mit der Cyberversicherung: Wie Unternehmen die komplexen Risiken besser verstehen und absichern können

Um die Herausforderungen der Cyber-Risikobewertung zu bewältigen, ist ein umfassender Ansatz erforderlich, der qualitative und quantitative Methoden kombiniert, die Schwächen traditioneller Risikobewertungen überwindet und trotzdem in einem für Unternehmen jeder Größenordnung durchführbarem Rahmen bleibt.

Downloaded from PwC Blogs on 04.12.2025 10:40h

Cyber-Bedrohungen sind vielfältig, immateriell und hochkomplex. Sie stellen sowohl für Unternehmen als auch für Versicherer erhebliche Herausforderungen dar, da sie sich grundlegend von traditionellen, versicherbaren Risiken unterscheiden. Ein wesentlicher Unterschied besteht darin, dass klassische Risiken—wie Naturkatastrophen oder Sachschäden—klar definierbare Ursachen und geografische Grenzen haben. Sie lassen sich in der Regel anhand historischer Daten und Erfahrungswerte relativ gut abschätzen und modellieren. Cyber-Risiken hingegen sind auf den ersten Blick „unsichtbar“, dynamisch und entwickeln sich ständig weiter, getrieben durch neue Technologien, sich verändernde Angriffsvektoren und oft unvorhersehbare Angriffsmethoden[1].

Cyber-Risiken umfassen ein breites Spektrum von Bedrohungen, darunter gezielte Phishing- und Ransomware-Angriffe, bei denen Cyberkriminelle über betrügerische E-Mails oder Schadsoftware Zugang zu sensiblen Daten erlangen wollen, sowie Insider-Bedrohungen durch Mitarbeiter:innen, die absichtlich oder unabsichtlich vertrauliche Informationen preisgeben. Hingegen zielen Distributed-Denial-of-Service (DDoS)-Angriffe darauf ab, Unternehmensnetzwerke zu überlasten und den Geschäftsbetrieb zu stören oder Schnittstellen zu digitalen Vertriebskanälen und Kundenportalen auszuschalten. Die Auswirkungen solcher Angriffe sind oft weitreichend und umfassen Betriebsunterbrechungen, erhebliche finanzielle Verluste, Reputationsschäden und regulatorische Konsequenzen.

Die Quantifizierung und Bewertung dieser Risiken ist besonders herausfordernd, da fehlende historische Daten, ständig wechselnde Angriffsmuster und die dynamische Natur des Bedrohungsumfelds herkömmliche Bewertungsmethoden bedingt aussagefähig machen[2]. Zudem sind die potenziellen Schäden oft nicht linear oder vorhersehbar, was die Bestimmung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmaßes erheblich erschwert.

Trotz dieser Schwierigkeiten existieren bereits Ansätze, die Unternehmen dabei unterstützen, ihre Cyber-Risiken genauer zu bewerten. Ein Beispiel hierfür ist die FAIR-Methode (Factor Analysis of Information Risk), die ein standardisiertes Modell zur Bewertung von Informationsrisiken bietet und es ermöglicht, Cyber-Risiken in einem strukturierten Rahmen zu quantifizieren und zu analysieren[3]. Dennoch ist es für viele Unternehmen herausfordernd ihr tatsächliches Risiko effizient zu bewerten und zu quantifizieren, was schlussendlich oft zu Unsicherheiten bei der Auswahl geeigneter Versicherungsdeckungen oder anderer Maßnahmen zur Risikominderung führt. In diesem Text stellen wir daher einen praxisorientierten Ansatz vor, der Unternehmen dabei unterstützen soll, ihre Cyber-Risiken systematisch zu analysieren, potenzielle Deckungslücken zu identifizieren und effektive Strategien zur Risikominderung und Absicherung zu entwickeln.

Problemdefinition

Reduziert man das Problem der Cyber-Risikobewertung auf seine wesentlichen Aspekte, lassen sich zwei entscheidende Fragen formulieren: **"Wie hoch ist der potenzielle Schaden, den ein Cyberangriff verursachen könnte?"** und **"Wie wahrscheinlich ist es, dass ein solcher Angriff in den kommenden Monaten eintritt?"**

Downloaded from PwC Blogs on 04.12.2025 10:40h

In der Praxis findet man häufig, dass die angewandten Methoden zur Risikobewertung von Cyber-Bedrohungen zu generisch oder abstrahiert sind und berücksichtigen somit nicht die spezifischen Auswirkungen, denen ein Unternehmen tatsächlich ausgesetzt ist. Beispiele hierfür sind vordefinierte Risikomatrizen, die auf alle Unternehmensrisiken gleichermaßen angewendet werden, oder einfache Schätzungen, die auf historischen Durchschnittswerten beruhen.

In einem Marktumfeld, in dem Versicherer zunehmend strenger und selektiver bei der Vergabe von Deckungen werden, ist eine fundierte und spezifische Risikobewertung jedoch umso wichtiger.

Ein Ansatz zur effizienten Risikoquantifizierung

Um die Herausforderungen der Cyber-Risikobewertung zu bewältigen, ist ein umfassender Ansatz erforderlich, der qualitative und quantitative Methoden kombiniert, die Schwächen traditioneller Risikobewertungen überwindet und trotzdem in einem für Unternehmen jeder Größenordnung durchführbarem Rahmen bleibt. Da die Möglichkeiten von Angriffen zahllos und die Kapazitäten begrenzt sind sollte sich das Unternehmen bei seiner Evaluierung gezielt auf Szenarien konzentrieren, welche aufgrund der aktuellen Bedrohungslage als auch aufgrund des Risikoprofils des Unternehmens als besonders relevant eingeschätzt werden können.

Beurteilung des eigenen Reifegrades:

Der Prozess beginnt mit einer indikativ angelegten Reifegradbewertung des Unternehmens, die den aktuellen Stand seiner Cybersicherheit erfasst. Diese Bewertung konzentriert sich auf zentrale Faktoren wie die Sicherheitskonfiguration von Netzwerken, den Schutz sensibler Daten, die Schulung der Mitarbeiter:innen und vorhandene Sicherheitszertifizierungen wie bspw. ISO 27001 oder die Einhaltung von branchenrelevanten Standards wie dem NIST Cybersecurity Framework[4,5]. Sie bietet eine erste Orientierung zu potenziellen Schwachstellen, etwa fehlenden Sicherheitsrichtlinien für Remote-Arbeit oder MFA (Multi-Faktor-Authentifizierung). Die daraus gewonnenen Ergebnisse ermöglichen eine initiale Einschätzung der Eintrittswahrscheinlichkeiten verschiedener Bedrohungsszenarien, wie die Gefahr von Phishing-Angriffen auf schlecht geschulte Mitarbeiter:innen, und dienen als Ausgangspunkt für die weiterführende Analyse.

Szenarienbasierte Analyse:

Um die potenzielle Eintrittswahrscheinlichkeit zu konkretisieren, wird ein speziell auf das Unternehmen zugeschnittener Set von Angriffsszenarien entwickelt. Kern der Modellierung liegt hierbei auf das angegriffene Asset (z.B. eine Datenbank oder eine Produktionsanlage), des Angriffs Vektors sowie den zu erwarteten Fähigkeiten/Ressourcen des Angreifers. Diese Szenarien sind repräsentativ für mögliche Bedrohungen, basierend auf der Branchenzugehörigkeit, bisherigen Vorfällen und aktuellen Schwachstellenprofilen des Unternehmens. Jedes Szenario wird einem Scoring unterzogen, das auf dem ermittelten Reifegrad der Cybersicherheit des Unternehmens aufbaut und verschiedene Faktoren (organisatorische wie technische) berücksichtigt, die die Wahrscheinlichkeit eines erfolgreichen Angriffs beeinflussen.

Downloaded from PwC Blogs on 04.12.2025 10:40h

Diese Szenarien können gezielte Phishing-Angriffe umfassen, bei denen Mitarbeiter:innen sensible Informationen preisgeben, Ransomware-Angriffe, die den Geschäftsbetrieb lahmlegen, Insider-Bedrohungen durch unzufriedene Mitarbeiter:innen oder Angriffe auf kritische Infrastrukturen wie die Unternehmensdatenbanken[6].

Betrachten wir einen erfolgreichen Ransomware-Angriff, der das zentrale ERP-System eines Unternehmens verschlüsselt und unzugänglich macht. Ein solcher Angriff würde den gesamten operativen Betrieb erheblich beeinträchtigen: Bestellungen könnten nicht bearbeitet, Lagerbestände nicht verwaltet und Rechnungen nicht erstellt werden. Die IT-Abteilung müsste sofort umfassende Maßnahmen zur Schadensbegrenzung und Systemwiederherstellung ergreifen. Dies würde nicht nur erhebliche personelle Ressourcen binden, sondern auch hohe Kosten für externe Spezialisten verursachen, die zur Entschlüsselung und Absicherung der Systeme benötigt würden. Gleichzeitig wäre der Zugriff auf buchhalterische Daten blockiert, was zu verzögerten Zahlungen und entgangenen Einnahmen führen könnte. Hinzu kämen Reputationsschäden, da die Geschäftsunfähigkeit Kunden und Partnern mitgeteilt werden müsste, was das Vertrauen in die Sicherheitsvorkehrungen des Unternehmens erschüttern könnte.

Die Simulation und Durchsprache solcher Angriffsvektoren ermöglicht eine differenzierte Bewertung der Schadensverläufe, da Fachkräfte wie IT-Experten und Controller eine präzisere Vorstellung von den Auswirkungen auf betroffene Bereiche, Systeme und Prozesse entwickeln. Dadurch wird eine fundierte Abschätzung der potenziellen Kosten in verschiedenen Schadensdimensionen ermöglicht, einschließlich Betriebsunterbrechungen und der Wiederherstellung kompromittierter Daten.

Für eine umfassende Analyse ist es essenziell, alle potenziellen Auswirkungen strukturiert zu erfassen. Hierbei werden alle relevanten Kostentreiber—Betriebsunterbrechungen, Datenverluste, Reputationsschäden oder regulatorische Auflagen—systematisch entlang der definierten Szenarien analysiert. Diese Herangehensweise ermöglicht es, transparente und nachvollziehbare Ergebnisse zu generieren, die auf fundierten, unternehmensinternen Daten basieren und realistische Werte widerspiegeln.

Vom Einzelfall zur Schadenverteilung:

Um eine fundierte Grundlage für die Risikobewertung zu schaffen, müssen potenzielle Schäden durch geeignete statistische Modelle und stochastische Verfahren realitätsnah abgebildet werden. Die bloße Aggregation von Schadensbeträgen greift zu kurz, da sie die inhärente Unsicherheit und die vielfältigen Einflussfaktoren, die die Schadenshöhe bestimmen, nicht ausreichend berücksichtigt. Stattdessen müssen unterschiedliche Schadensausmaße und deren Eintrittswahrscheinlichkeiten mittels probabilistischer Ansätze modelliert werden, um eine valide und belastbare Schadenverteilung zu erzeugen.

Insbesondere die Monte-Carlo-Simulation hat sich in der Praxis als geeignete Methode zur Quantifizierung von Cyber-Risiken erwiesen[7]. Durch die Durchführung einer großen Anzahl von Zufallssimulationen können unterschiedliche Eintrittswahrscheinlichkeiten und Schadensausprägungen—etwa bei verschiedenen Angriffsszenarien wie Phishing oder Ransomware—systematisch berücksichtigt werden. Dies generiert eine Vielzahl möglicher Ergebnisse und ermöglicht eine umfassende, probabilistisch fundierte Analyse der

Downloaded from PwC Blogs on 04.12.2025 10:40h

Risikoverteilung. Auf diese Weise kann das Unternehmen evaluieren, inwieweit aktuelle oder geplante Versicherungslösungen ausreichend sind, um das identifizierte Risikopotenzial abzudecken, und gegebenenfalls Anpassungen vornehmen, um Deckungslücken zu schließen.

Nach dem Assessment ist vor dem Assessment

Ein einmal durchgeführtes Cyber-Risiko-Assessment liefert wertvolle Einblicke, doch die Dynamik des digitalen Umfelds erfordert eine regelmäßige Wiederholung. Die kontinuierliche Neubewertung ermöglicht es, den Detailgrad zu erhöhen und auf den gewonnenen Erkenntnissen aufzubauen. Jede Iteration trägt zur Präzisierung der Risikoanalyse bei und verbessert die Entscheidungsgrundlage für Risikomanagementstrategien.

Die Praxiserfahrung zeigt zudem, dass beteiligte Personen eine steile Lernkurve durchlaufen. Wenn Key Accountmanager, IT-Experten und Security Mitarbeiter:innen gemeinsam die Ausmaße möglicher Unterbrechungen und notwendiger Mitigationsmaßnahmen analysieren kommt es häufig zu überraschenden Erkenntnissen, die das tatsächliche Risikoprofil des Unternehmens vervollständigen. Mit zunehmender Erfahrung können außerdem spezifische Fragestellungen gezielter adressiert werden. Beispielsweise erweist sich die Bewertung von Reputationsschäden oft als komplex und schwer vorhersehbar. Durch wiederholte Assessments entwickeln die Beteiligten ein tieferes Verständnis für dieses Thema und können fundiertere und präzisere Bewertungen vornehmen.

Diese fortlaufende Verbesserung der Expertise und die detailliertere Fokussierung auf spezifische Risiken tragen dazu bei, dass die Risikobewertungen im Laufe der Zeit immer umfassender und genauer werden.

Schlussfolgerungen und Empfehlungen

Eine präzise Quantifizierung von Cyber-Risiken ist für Unternehmen unerlässlich, um die Angemessenheit ihrer Versicherungsstrategien zu überprüfen und einen effektiven Schutz gegen Cyber-Bedrohungen zu gewährleisten. Außerdem werden Mitarbeiter:innen für das Thema stärker sensibilisiert und mit den gewonnenen Erkenntnissen die eigenen Resilience gestärkt. Der vorgestellte Ansatz bietet eine Grundlage, um spezifische Risiken zu bewerten und geeignete Maßnahmen zur Risikominderung und Absicherung zu identifizieren. Unternehmen sollten regelmäßig detaillierte Risikoanalysen durchführen und sowohl die Eintrittswahrscheinlichkeit als auch die finanziellen Auswirkungen potenzieller Angriffe berücksichtigen, um fundierte Entscheidungen zu treffen.

Für Unternehmen, die eine genaue Quantifizierung ihrer Cyber-Risiken anstreben und ihre Risikoabsicherung optimieren möchten, wird eine weitergehende Beratung empfohlen. Eine begleitete maßgeschneiderte Analyse und Bewertung kann dazu beitragen, die richtigen Entscheidungen zu treffen und besser gegen zukünftige Bedrohungen gewappnet zu sein.

---

[1]World Economic Forum. (2022).*Global Risks Report 2022*. Verfügbar unter: https://www.weforum.org/reports/global-risks-report-2022

[2]Ponemon Institute. (2023). *Cost of a Data Breach Report 2023*

Downloaded from PwC Blogs on 04.12.2025 10:40h

[3]FAIR Institute.*An Introduction to Factor Analysis of Information Risk (FAIR)*. Verfügbar unter: https://www.fairinstitute.org/

[4] International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*.

[5]National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Verfügbar unter: https://www.nist.gov/cyberframework

[6] Verizon. (2023). *Data Breach Investigations Report*. Verfügbar unter: https://www.verizon.com/business/resources/reports/dbir/

[7] Hubbard, D. W., & Seiersen, R. (2016). *How to Measure Anything in Cybersecurity Risk*. John Wiley & Sons

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

Schlagwörter

IT-Sicherheit, Risk Management Insurance

Kontakt

Dr. Alexander Dotterweich
München
alexander.dotterweich@pwc.com