06.24

KSI

Krisen-, Sanierungs- und Insolvenzberatung

20. Jahrgang
November/Dezember 2024
Seiten 241–288

www.KSIdigital.de

Wirtschaft
Recht
Steuern

ESV ERICH SCHMIDT VERLAG
100 Jahre

69037

Cyber Security als Erfolgsfaktor in der Restrukturierung

Praxisnahe Tipps und Checkpoints aus dem Interim Management für das Management und Restrukturierungsexperten

Andreas Lau*

In der digitalen Welt sind Unternehmen vielfältigen Bedrohungen durch Cyber-Angriffe ausgesetzt. Besonders *in Krisen- und Restrukturierungsphasen*, wenn Unternehmen finanziell unter Druck stehen, wird Cyber Security zu einem kritischen Thema. Cyber-Kriminelle machen sich die Schwachstellen von Unternehmen zunutze, deren IT-Infrastruktur oft veraltet ist oder deren Ressourcen zur Sicherung der Daten begrenzt sind. Die Auswirkungen von Cyber-Angriffen auf Unternehmen können verheerend sein und reichen von Produktionsausfällen über Datenverluste bis hin zur Existenzbedrohung und Insolvenz. Dieser Artikel beleuchtet die Bedeutung von Cyber Security in Restrukturierungssituationen und gibt *praxisorientierte Empfehlungen für Unternehmer, (Interim) Manager und (Sanierungs-)Berater*, die Cyber-Risiken beurteilen und Cyber Security managen müssen – erfahrungsgemäß häufig, ohne ausgebildete Experten auf diesem Gebiet zu sein.

1. Manager als Cyber-Schutzschild

Cyber-Angriffe sind laut aktuellen Unternehmerumfragen das Top-Risiko 2024. Die Schadensfälle sind um 50 % zum Vorjahr gestiegen. 2023 haben die Schäden 206 Mrd. € allein in Deutschland betragen. Von Angriffen betroffen ist in Deutschland der Stückzahl nach hauptsächlich der Mittelstand. Jeder Cyber-Angriff birgt das Risiko eines Totalverlustes des Unternehmens. Etwa 20 % von einem Cyber-Angriff betroffene Unternehmen sahen sich am Rande der Insolvenz. Da es ein größeres unternehmerisches Risiko kaum gibt, sind Maßnahmen wie umfassende Schulungen[1] umso wichtiger – nachfolgend wird dies aus der Sicht des Interim Managements näher begründet.

1.1 Wahrnehmung der Bedrohungen

Aus dieser Brille müssen auch Eigenkapitalgeber wie Fremdfinanzierer auf das Schutzbedürfnis des Unternehmens vor diesem Risiko schauen. Die Awareness bei allen Stakeholdern des Unternehmens erfasst aber i. d. R. noch nicht die Tragweite des Risikos. Zwar steigen die Investitionen in Cyber Security, sind aber meist noch zu niedrig. Versicherungen werden deutlich teurer. Unternehmen werden nur noch mit hohen Auflagen an Cyber-Security-Standards überhaupt versichert. Und Versicherer zahlen im Schadensfall beileibe nicht immer den Gesamtschaden.

Finanzierer müssen sich im Klaren sein: Das Ausfallrisiko des Gesamtkredits ist ein reales Bedrohungsszenario bei Cyber-Angriffen. Deshalb ist seit kurzem auch die Beurteilung des Cyber-Security-Managementsystems Bestandteil des IDW-S6-Gutachtens.

Organe des Unternehmens, die die Implementierung eines Cyber-Security-Managementsystems stiefmütterlich behandeln, setzen sich erheblichen (persönlichen) Haftungsrisiken aus. Etwa zehn verschiedene Gesetze enthalten Bestimmungen, um den nachlässigen Geschäftsführer in Haft zu nehmen.

1.2 Technologische Bedrohungserkennung und -abwehr durch KI

Der Einsatz von Künstlicher Intelligenz (KI) zur Erkennung von Angriffen und Angriffsarten wird zunehmend wichtiger. Im Wirkungsbereich des Verfassers werden Interim Manager in der Schulung darauf vorbereitet, welche modernen Tools sie nutzen können, um Bedrohungen proaktiv zu erkennen. KI kann dabei helfen, Anomalien im Netzwerkverkehr frühzeitig zu identifizieren und Maßnahmen zu ergreifen, bevor größerer Schaden entsteht.

1.3 Prävention und Reaktion – von Notfallplänen bis zum Incident Management

Eines der Schlüsselelemente in der Cyber-Security-Schulung ist die Installation eines Cyber-Security-Managementsystems, wo ohne Zweifel die Entwicklung und Implementierung von Notfallplänen eine zentrale Rolle mit vielen Teilelementen spielt. Diese Pläne beinhalten genaue Schritte, wie im Falle eines Angriffs vorzugehen ist, um den Schaden zu minimieren. Das Incident-Management umfasst fünf Phasen (vgl. im Überblick Abb. 1, S. 266): Vorbereitung, Detektion, Eindämmung, Wiederherstellung und die Nachbereitung (Lessons Learned). Jede Phase ist entscheidend, um den Betrieb schnell wiederherzustellen und künftige Angriffe besser abwehren zu können. Die Lückenlosigkeit des Managementsystems ist auch wesentlich für den Schadensausgleich durch den Versicherer und sie ist unverzichtbar für die (persönliche) Enthaftung des Geschäftsführers.

Bei Lösegeldforderungen scheiden sich die Geister: Zahlen oder nicht – mindestens so

* Andreas Lau ist geschäftsführender Partner der HANSE Interim Management GmbH. Neben der Vermittlung von Interim Managern hat er sehr umfassende Erfahrung aus rund 200 persönlich verantworteten Mandaten als Unternehmensberater oder Interim Manager (CRO) in den Bereichen Sanierung, Restrukturierung, Transformation, Ertragssteigerung und M&A. Seit fast 25 Jahren ist HANSE Interim führend im Qualitäts-Interim-Management und spezialisiert auf die kurzfristige Besetzung von interimistischen Führungspositionen sowie das Management kritischer, auch insolvenznaher Projekte. Mit einem Pool von über 3500 hochqualifizierten Interim Managern (darunter ca. 100 CROs) aus 30 Funktionsbereichen und mehr als 280 Branchen bietet HANSE Interim umfassende Experten für eine Vielzahl von interimistischen Personalbedarfen in unterschiedlichsten Unternehmenssituationen.

1 Beispielsweise wird bei HANSE Interim großer Wert darauf gelegt, dass sich seine Interim Manager umfassend fortbilden, um im Ernstfall effektiv reagieren zu können. Die Cyber-Security-Schulung ist praxisorientiert und integriert reale Fallbeispiele aus der Unternehmenswelt. In dieser Fortbildung lernen Manager, wie sie Lücken im Cyber-Security-Managementsystem entdecken, Cyber-Angriffe schnell erkennen und wie sie effektive Schutz- und Gegenmaßnahmen definieren und umsetzen.

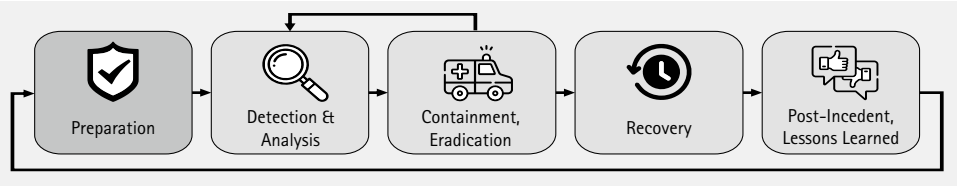

Abb. 1: Incident-Management

viele Experten raten davon ab wie es Fürsprecher zur Zahlung gibt. Dafür spricht die Hoffnung auf den Wiedererhalt der Daten, aber dagegen auch das Funding und Stärken der angreifenden Organisationen und Staaten.

1.4 Finanzielle Schäden und Versicherungsaspekte

Cyber-Angriffe haben oft gravierende finanzielle Auswirkungen. Besonders zu Buche schlagen in der Reihenfolge nach dem durchschnittlichen Wert: Imageschäden, Ausfall der Produktion, Rechtsstreitigkeiten, Forensik und Ermittlungen, Umsatzausfälle, Patentrechtsverletzungen. 206 Mrd. € finanzielle Schäden allein in Deutschland wollen gut versichert sein.

Interim Manager müssen wissen, was überhaupt versicherbar ist und was nicht. In Abhängigkeit vom Geschäftsmodell und der Risikobeurteilung müssen die richtigen Versicherungsbausteine gewählt werden. Und mindestens genauso wichtig sind Antworten auf folgende Fragen:

- In regelmäßigen Abständen muss der adäquate Versicherungsschutz überprüft werden. Sind Anpassungen erforderlich?
- Welche Dokumentations- und Meldepflichten bestehen? Was ist zu tun im Schadensfall?

2. Rechtliche Hintergründe

Beispiele für häufige, aber typische (rechtliche) Irrtümer des Managements lassen sich wie folgt nennen:

- Der „Versicherungsrechtler“: „Cyber-Risiken – dafür haben wir doch eine Cyber-Versicherung“.
- Der „Exkulpationsrechtler“: „Das ist Sache der IT“.
- Der „Aufgebende Rechtler“: „Wir sind zu klein, um etwas dagegen zu tun“.
- Der „Minimalrechtler“ oder der „Maximalrechtler“? „Wir erfüllen den Mindeststandard, das reicht“.

Cyber-Sicherheitsrecht gleicht einer Puzzelei oder einem Flickenteppich? Etwa zehn Rechtsgebiete streifen oder definieren das Cyber-Sicherheitsrecht. Abb. 2 zeigt eine Auswahl.

Gem. Aktiengesetz und GmbH-Gesetz (AktG/GmbHG) ergibt sich die Pflicht des Vorstands oder Geschäftsführers zur sorgfältigen Unternehmensleitung. Es besteht die Pflicht zur Installierung eines angemessenen, internen Risikomanagements für Gesellschaften. Die Geschäftsführung verantwortet die IT-Sicherheit – mit allen Konsequenzen (z. B. Schutz vor Cyber-Angriffen). Kernaufgabe der Geschäftsführung ist die Bestimmung und Vorbereitung der angemessenen Reaktion (z. B. auf Cyber-Angriffe). Nur wenn die Geschäftsführung nachweislich alle geforderten sicherheitsrelevanten Maßnahmen umgesetzt hat, kann sie sich aus der Haftung im Schadenfall exkulpieren (also doch besser Installation eines „maximalen“ Cyber-Security-Managementsystems).

Zu beachten ist ferner § 25a KWG Kreditwesengesetz, wonach die „Festlegung eines angemessenen Notfallmanagements, insbesondere für IT-Systeme“ erforderlich ist. Im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) heißt es, dass der rechtliche Schutz von wirtschaftlich relevanten Unternehmensinformationen nach § 2 Nr. 1b angemessene Geheimhaltungsmaßnahmen voraussetzt. Dies erfordert die Kennzeichnung von Informationen als vertraulich, vertragliche Vereinbarungen zum Geheimnisschutz (etwa mit Arbeitnehmern oder Dritten) sowie eine Verschlüsselung/Passworte.

Gem. der DSGVO müssen personenbezogene Daten vor unbefugter Verarbeitung, Verlust und Zerstörung geschützt werden. Dabei sind gängige Standards einzuhalten (Art. 32 DSGVO). Orientierung bieten z. B. *IT-Grundschutzkataloge* des BSI.

Im IT-Sicherheitsgesetz 2.0 ist die Pflicht festgeschrieben, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der *Verfügbarkeit*, Integrität, Authentizität und *Vertraulichkeit* zu treffen (§ 8a Abs. 1 BSIG). Vorausgesetzt wird die Einhaltung des Stands der Technik, insbesondere auch durch *branchenspezifische* Sicherheitsstandards.

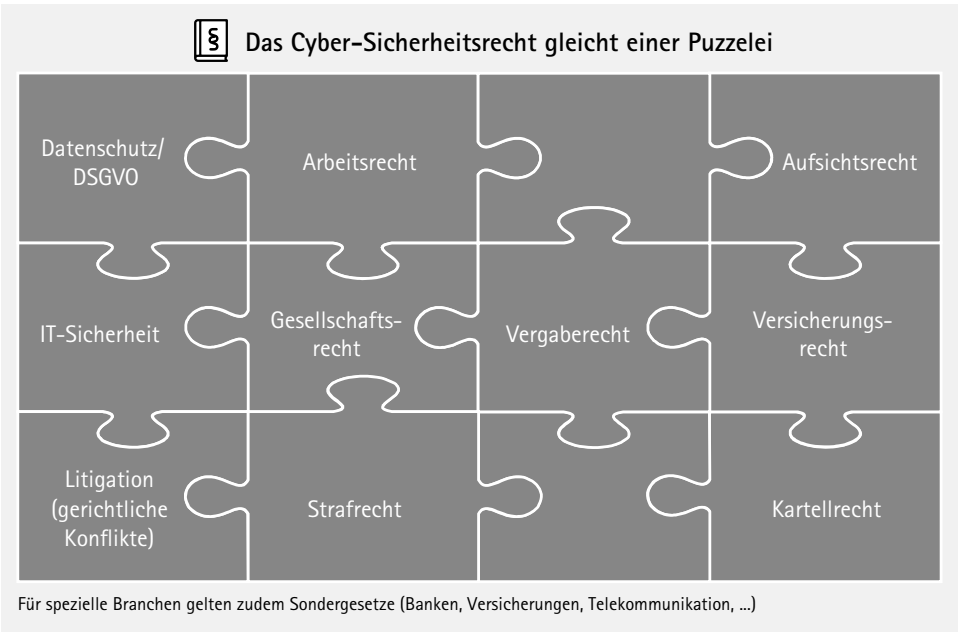

Abb. 2: Cyber-Sicherheitsrecht

Ferner ergeben sich aus dem Arbeitsrecht/Betriebsverfassungsrecht die folgenden Anforderungen:

- Beim Einsatz von Cyber-Security-Tools sind regelmäßig – wenn auch nicht ausschließlich – personenbezogene Daten betroffen. Hierzu ist die Erlaubnis der betroffenen Mitarbeiter erforderlich (§ 4 Abs. 1 BDSG).
- Zudem sind solche Tools oftmals zur Kontrolle von Verhalten und Leistung der Arbeitnehmer geeignet (Log-Dateien), auch wenn dies nicht das primäre Ziel der Tools ist. Hierdurch wird das Mitbestimmungsrecht ausgelöst.
- Die Mitbestimmung des Betriebsrats ist beim Einsatz von Überwachungs-Software besonders weitreichend (§ 87 Abs. 1 Nr. 6 BetrVG).
- Mitarbeiter sind zur Abwehr von Schäden verpflichtet und müssen Maßnahmen ergreifen, um Arbeitgeber zu schützen: Pflicht zur Teilnahme an Backups, Unterbrechung von externen Verbindungen etc.

Insgesamt gesehen muss beachtet werden, dass nicht nur den Cyber-Angreifern Konsequenzen drohen. Auch das angegriffene Unternehmen und Management kann hohe Bußgelder treffen, wenn es Versäumnisse bei den vorgeschriebenen Vorkehrungen gab.

3. Die Cyber-Security-Checkliste zur Bestandsaufnahme und Steuerung der Maßnahmenumsetzung

3.1 Werkzeug auch im Krisenmanagement

Die von HANSE Interim angewendete Cyber-Security-Checkliste ist ein wichtiges Tool, um (Interim) Managern und Beratern zu helfen, potenzielle Schwachstellen in der IT-Sicherheitsarchitektur eines Unternehmens schnell zu identifizieren und zu beheben. Diese Checkliste wurde speziell für Manager entwickelt, die eine Bestandsaufnahme durchführen müssen oder in Krisen- oder Restrukturierungsprozessen arbeiten und sich nicht immer intensiv mit technischen Details auseinandersetzen können. Sie sollen schnell in die Bestandsaufnahme kommen, insbesondere auch, wenn sie in eigener Haftung stehen ab dem ersten Tag des Engagements, aber auch für Restrukturierungsberater, die das Cyber-Security-Managementsystem schnell beurteilen müssen.

Abb. 3: Risikosenkung durch Prävention und Reaktion

In Abschn. 3.2 sind die wichtigsten Punkte aufgelistet, die die Checkliste [2] abdeckt (vgl. im Überblick Abb. 3).

3.2 Einzelbetrachtung der Checklisten-Maßnahmen

3.2.1 IT-Sicherheitsverantwortliche bestimmen

Eine der ersten Maßnahmen besteht darin, klare Zuständigkeiten für die IT-Sicherheit zu definieren. Dies ist besonders wichtig in Restrukturierungsprozessen, in denen Ressourcen knapp sind und Verantwortlichkeiten neu verteilt werden müssen. Unternehmen sollten sicherstellen, dass sie ein definiertes IT-Sicherheitsteam oder zumindest eine verantwortliche Person haben, die die Überwachung der Cyber Security übernimmt. Regelmäßige Sicherheitsüberprüfungen, Schulungen und die Koordination der Abwehrmaßnahmen sind essenziell.

Praxisbeispiel: Ein mittelständisches Produktionsunternehmen, das sich in einer Restrukturierung befand, erlitt einen schweren Cyber-Angriff durch Ransomware. Da die IT-Verantwortlichkeiten nach einer internen Umstrukturierung unklar waren, dauerte die Reaktion auf den Angriff viel zu lange. Ein klar definiertes IT-Sicherheitsteam hätte den Schaden deutlich schneller und entscheidungssicherer bearbeiten und damit minimieren können.

3.2.2 Regelmäßige Wartung und Updates von IT-Systemen

Veraltete Software und Systeme bieten eine der größten Angriffsmöglichkeiten für Hacker. Unternehmen sollten ihre IT-Systeme regelmäßig aktualisieren und Wartungen einplanen, um bekannte Sicherheitslücken zu schließen. Besonders in der Restrukturierung kann der Druck, Kosten zu senken, dazu führen, dass IT-Sicherheitsinvestitionen vernachlässigt werden.

Ein zentraler Aspekt hierbei ist das Management von sog. *Zero-Day-Exploits* – Schwachstellen, die von Angreifern ausgenutzt werden, bevor der Softwareanbieter ein Update zur Schließung bereitstellen kann. Auch Unternehmen in der Restrukturierung sollten unbedingt sicherstellen, dass ihre Systeme regelmäßig auf solche Schwachstellen überprüft und gepatcht werden.

3.2.3 Backup-Strategien und deren Umsetzung

Die Durchführung regelmäßiger Backups ist eine der grundlegendsten Sicherheitsmaßnahmen, die ein Unternehmen ergreifen kann (vgl. Abb. 4). In Restrukturierungsprozessen besteht jedoch oft das Risiko, dass Backups vernachlässigt oder nicht systematisch durchgeführt werden. Dabei sollten Unternehmen mindestens wöchentliche

2 Zum Abruf per E-Mail an den Verfasser: Lau@hanse-interimmanagement.de.

Backups ihrer Daten vornehmen und sicherstellen, dass diese an einem sicheren Ort gespeichert werden – am besten außerhalb des Firmennetzwerks.

Praxisbeispiel: Ein international tätiges Handelsunternehmen, das sich in einem Restrukturierungsprozess befand, wurde Opfer eines Ransomware-Angriffs. Da es jedoch regelmäßig Backups durchführte, konnte das Unternehmen seine Daten schnell wiederherstellen und den Betrieb innerhalb weniger Tage fortsetzen. Ohne die Backups hätte ein monatelanger Stillstand gedroht.

Regelmäßige Datensicherung ist beileibe keine Selbstverständlichkeit: Noch 2021 machten nur 50 % der befragten Unternehmen mindestens wöchentlich eine Datensicherung[3]. Es sind Fälle bekannt, wo Unternehmen direkt in die Insolvenz gegangen sind, da ihr gesicherter Datenbestand zu alt war, um einen geordneten Betrieb nach einem Angriff wieder aufnehmen zu können.

3.2.4 Passwort- und Zugangsberechtigungspolitik

Unsichere Passwörter und unzureichende Zugriffskontrollen stellen eine der häufigsten Ursachen für erfolgreiche Cyber-Angriffe dar. In Zeiten von Umstrukturierungen und Personalwechseln kann es zu Lücken in den Zugriffsberechtigungen kommen, die Angreifer ausnutzen. Eine strikte Passwortpolitik und regelmäßige Überprüfung der Zugriffsrechte sind unerlässlich. Dies gilt besonders für sensible Unternehmensbereiche wie Finanzabteilungen mit Zugang zu Kundendaten sowie Forschungs- und Entwicklungsbereiche.

3.2.5 Firewalls, Virenschutzsysteme und Netzwerküberwachung

Unternehmen sollten nicht nur Virenschutzprogramme, sondern auch Firewalls und Intrusion Detection Systeme (IDS) einsetzen, um verdächtige Aktivitäten frühzeitig zu erkennen und um den Zugang zu sensiblen Daten zu kontrollieren. Diese Systeme sollten regelmäßig aktualisiert und durch ein Netzwerküberwachungssystem ergänzt werden, das verdächtige Aktivitäten frühzeitig erkennt, ansonsten können viele Bedrohungen erst erkannt werden, wenn es zu spät ist.

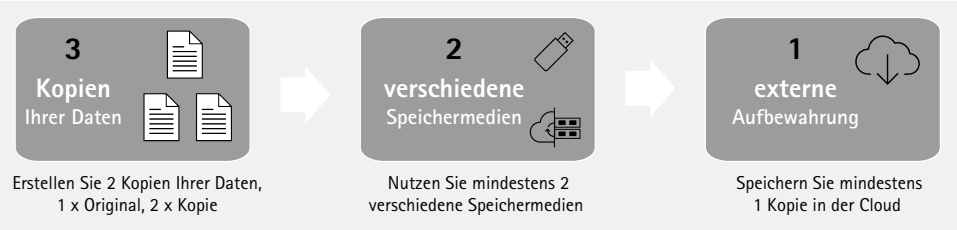

Abb. 4: Backup-Strategie (z. B. 3–2-1-Regel)

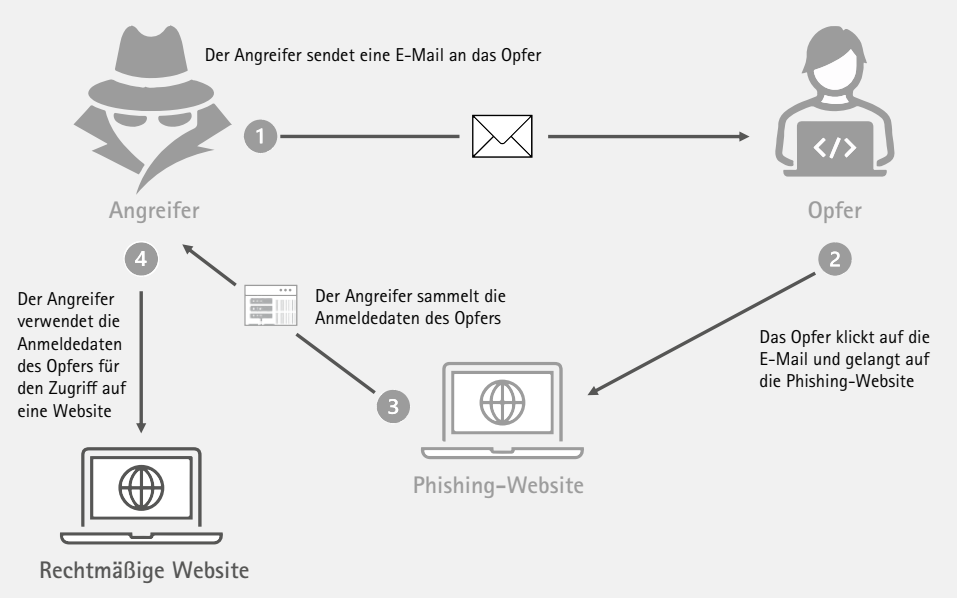

Abb. 5: Typischer Phishing-Angriff

3.2.6 Externe Geräte

Daten auf externen Geräten (Laptops, Smartphones, USB-Laufwerke) müssen vor Verlust oder Diebstahl geschützt sein. Zu fragen ist:

- Sind Maßnahmen zur Verschlüsselung, Passwortschutz und Remote-Löschung implementiert?
- Welche Restriktionen zur Nutzung externer Geräte gibt es (z. B. USB-Sticks)?

3.2.7 Schulung und Sensibilisierung der Mitarbeiter

Auch die besten technischen Schutzmaßnahmen können unterlaufen werden, wenn Mitarbeiter unsicher im Umgang mit potenziellen Bedrohungen sind. Phishing-Angriffe, bei denen Mitarbeiter durch täuschend echt aussehende E-Mails dazu gebracht werden, vertrauliche Informationen preiszugeben, sind nach wie vor eine der häufigsten Angriffsarten (vgl. Abb. 5). Schulungen helfen, das Bewusstsein für diese Bedrohungen zu schärfen und entsprechende Reaktionen zu trainieren.

Gerade in Zeiten der Restrukturierung, in denen Verunsicherung im Unternehmen herrscht, kann die Wachsamkeit der Mitarbeiter nachlassen. Regelmäßige Mitarbeiterschulungen sind sehr zu empfehlen.

3.2.8 Versicherungsschutz gegen Cyberrisiken

Angesichts der zunehmenden Bedrohungslage haben viele Unternehmen Cyber-Versicherungen abgeschlossen, um sich gegen die wirtschaftlichen Folgen eines Angriffs zu schützen, andere nicht. In Restrukturierungsphasen, in denen das finanzielle Risiko ohnehin hoch ist, sollte geprüft werden, ob der Versicherungsschutz ausreichend ist. Im Schadensfall wird dann die Kreditlinie nicht (vollumfänglich) durch den Schaden belastet.

3 Quelle: Infofact, Umfrage 12/2021 bei 511 Entscheidern im deutschen Mittelstand.

3.2.9 Notfall- und Wiederherstellungskonzepte

Im Ernstfall zählt jede Minute. Unternehmen sollten klar definierte Notfallpläne für den Fall eines Cyber-Angriffs haben, die beschreiben, wie sie auf den Angriff reagieren und die Auswirkungen minimieren können. Ein effektives Incident-Management-Protokoll hilft, den Betrieb schnell wiederherzustellen.

4. Unternehmen in der Restrukturierung

4.1 Besondere Anfälligkeit für Cyber-Angriffe

Wenn Unternehmen sich in einer Restrukturierung befinden, liegt der Fokus häufig auf der Stabilisierung von Finanzen und Geschäftstätigkeit. Der IT-Sicherheit wird dabei oft weniger Beachtung geschenkt – eine gefährliche Lücke, die von Cyberkriminellen ausgenutzt werden kann. In solchen Phasen sind viele Unternehmen gezwungen, kurzfristige Entscheidungen zu treffen, die nicht immer den langfristigen Schutz der IT-Systeme berücksichtigen. Hinzu kommt, dass finanziell angeschlagene Unternehmen oft nicht über die Mittel verfügen, um in modernste Sicherheitslösungen zu investieren.

Statistiken belegen, dass Unternehmen, die in *Restrukturierungsprozesse* involviert sind, einem bis zu *50 % höheren Risiko* ausgesetzt sind, Opfer von Cyber-Angriffen zu werden[4]. Diese Angriffe sind nicht nur eine Bedrohung für den laufenden Betrieb, sondern können auch die gesamten Restrukturierungsbemühungen gefährden, da sie wichtige Geschäftsdaten und -systeme lahmlegen.

Unternehmen in der Restrukturierung sind aus mehreren Gründen besonders gefährdet. Die IT-Infrastruktur dieser Unternehmen ist oft veraltet und bietet daher eine größere Angriffsfläche. Hinzu kommt, dass finanzielle Engpässe die Möglichkeit einschränken, in präventive Sicherheitsmaßnahmen zu investieren. Zudem kann die allgemeine Unsicherheit und Unruhe im Unternehmen dazu führen, dass Mitarbeitende weniger wachsam sind und Sicherheitsrichtlinien vernachlässigen.

4.2 Wirtschaftliche und rechtliche Folgen von Cyber-Angriffen als Bedrohung für die Restrukturierung

Cyber-Angriffe stellen nicht nur eine technische Herausforderung dar, sondern bergen auch immense wirtschaftliche und rechtliche Risiken. Insbesondere in Restrukturierungsphasen kann ein Cyber-Angriff das Unternehmen in den Ruin treiben. In vielen Fällen führt der Verlust von Kundendaten oder der Ausfall kritischer IT-Systeme zu Umsatzverlusten und Vertrauensverlust bei Kunden und Partnern. Eine Studie[5] aus dem Jahr 2023 zeigt, dass fast 60 % der Unternehmen, die von einem schweren Cyber-Angriff betroffen sind, auch langfristige wirtschaftliche Schäden davongetragen haben.

5. Fazit: Cyber Security als unverzichtbarer Bestandteil im Restrukturierungsplan

In Restrukturierungsprozessen wird oft der Fehler gemacht, Cyber Security als nachrangig zu betrachten. Doch gerade in Krisenzeiten ist es entscheidend, Cyber-Risiken systematisch zu managen und in den Restrukturierungsplan zu integrieren.

Die Integration von Cyber Security in Restrukturierungsprozesse ist also nicht mehr nur eine Option, sondern eine absolute Notwendigkeit. Die in Abschn. 3.2 skizzierte Checkliste und die umfassende Schulung helfen Managern dabei, Unternehmen sicher durch Krisenzeiten zu führen und vor den weitreichenden Gefahren von Cyber-Angriffen zu schützen.

Cyber Security ist außerdem ein kritischer Erfolgsfaktor in Restrukturierungsprozessen. Unternehmen, die sich in einer finanziellen Schieflage befinden, sind besonders anfällig für Cyber-Angriffe, und die Folgen solcher Angriffe können existenzbedrohend sein. Es ist daher unerlässlich, dass Cyber Security von Anfang an in den Restrukturierungsplan integriert wird. Dies erfordert nicht nur technische und organisatorische Maßnahmen, sondern auch eine enge Zusammenarbeit zwischen dem Management, IT-Sicherheitsexperten und Finanzierern.

Nur durch eine ganzheitliche Betrachtung und Integration von Cyber Security in die Unternehmensstrategie können das wirtschaftliche Risiko minimiert und das Vertrauen von Investoren und Stakeholdern gestärkt werden. Dabei gilt: Cyber Security ist Chefsache!

4 Vgl. zu entsprechenden statistischen Feststellungen diverse Studien und Befragungen. Z. B.: FINANCE mit SMP, 88 Experten, Restrukturierungsbarometer; oder diverse Bitkom-Studien, ca. 1.000 Unternehmen. Zielpersonen: Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind. Dazu zählen Geschäftsführer sowie Führungskräfte aus den Bereichen Unternehmenssicherheit, IT-Sicherheit, Risikomanagement oder Finanzen.

5 Bitkom Research; Wirschaftsschutz 2024.