Cyberrisiken und Insolvenzgefahr: Präventive Schutzpflichten des NIS2-Regimes

RA Dr. Dr. Fabian Teichmann, LL.M.

Cyberangriffe haben sich von einem reinen IT-Problem zu einem potenziellen Insolvenzrisiko entwickelt. Zahlreiche Praxisfälle – wie die Insolvenzen von Fasana (2025) und Schumag (2024) – verdeutlichen, dass Ransomware und andere Angriffe unmittelbar existenzbedrohend sein können. Vor diesem Hintergrund verpflichtet die NIS2-Richtlinie (EU) 2022/2555 eine breite Kategorie von Unternehmen zu präventiven Cybersicherheitsmaßnahmen und bindet erstmals auch die Geschäftsleitungen persönlich in die Verantwortung ein. Dieser Beitrag analysiert, wie Cybervorfälle insolvenzrechtlich relevant werden, welche konkreten Schutzpflichten NIS2 vorsieht und inwiefern deren Umsetzung geeignet ist, Insolvenzen vorzubeugen. Dabei wird gezeigt, dass NIS2 einen ganzheitlichen Ansatz verfolgt, der Unternehmen zu erhöhter Resilienz verpflichtet und damit als präventives Insolvenzschutzinstrument wirkt, auch wenn Lücken verbleiben.

1. Einleitung

Unternehmen sehen sich in der digitalen Wirtschaft einer stetig wachsenden Gefahr durch Cyberangriffe gegenüber. Die Zahl schwerwiegender IT-Sicherheitsvorfälle ist in den letzten Jahren rasant gestiegen. Ihre Folgen gehen längst über reine IT-Schäden hinaus und können für Unternehmen existenzbedrohend werden. Aktuelle Studien zeichnen ein alarmierendes Bild: So waren 2023 rund 72 % der deutschen Unternehmen von Cyberattacken betroffen, und der gesamtwirtschaftliche Schaden durch Datendiebstahl, Spionage und Sabotage wird auf 206–266 Milliarden Euro pro Jahr beziffert.[1] Mehr als die Hälfte der Unternehmen fühlt sich inzwischen durch Cyberangriffe in ihrer Existenz bedroht – 2023 erstmals 52 %, 2024 bereits 65 % (zum Vergleich: 2021 erst 9 %).[2] Diese Entwicklungen zeigen, dass Cyberrisiken längst insolvenzrelevante Bedeutung erlangt haben.

RA Dr. Dr. Fabian Teichmann, LL.M. (London), MBA (Oxford), Notar (St. Gallen), Managing Partner der Teichmann International (Schweiz) AG sowie Präsident des Verwaltungsrats der Teichmann International (IT Solutions) AG; Lehrbeauftragter und Autor zahlreicher Publikationen im Bereich Strafrecht, Wirtschaftsstrafrecht und Cybersecurity

Die Praxis bestätigt diese Sorge. Immer häufiger treiben Hackerangriffe selbst traditionsreiche Mittelstandsunternehmen in die Insolvenz. Ein prominentes Beispiel ist der Fall *Fasana*: Der über 100 Jahre alte Serviettenhersteller aus Euskirchen musste im Juni 2025 Insolvenz anmelden, nachdem ein Ransomware-Angriff die gesamte Produktion wochenlang lahmgelegt und rund 2 Millionen Euro Umsatzverlust verursacht hatte.[3] Ähnlich erging es der börsennotierten *Schumag AG* (Präzisionsteile-Hersteller, Aachen), die bereits in finanzieller Schieflage war und durch einen Cyberangriff im September 2024 endgültig in die Krise gedrängt wurde – unerwartete Produktionsausfälle und Verzögerungen führten zu akuten Liquiditätslücken, sodass das Unternehmen ein Sanierungs-

[1] Unternehmen Cybersicherheit, Bitkom-Studie: 52 Prozent der Unternehmen fühlen sich durch Cyberattacken in ihrer Existenz bedroht

[2] Bitkom, Angriffe auf die deutsche Wirtschaft nehmen zu

[3] FOCUS online: Wie ein Hackerangriff ein deutsches Traditionsunternehmen in die Insolvenz trieb; Stern.de: Erpresserbrief im Drucker: Hacker treiben Servietten-Fabrik in die Insolvenz; WDR.de: Euskirchener Serviettenfirma droht nach Cyberattacke Insolvenz

verfahren in Eigenverwaltung einleiten musste.[1] Diese Fälle sind keine Einzelfälle, sondern stehen exemplarisch für ein Phänomen, dass Cybervorfälle im schlimmsten Fall die Insolvenzauslöser sein können, sei es durch unmittelbare Betriebsunfähigkeit und Einnahmeausfälle oder durch Folgekosten (Wiederherstellungsmaßnahmen, Haftungs- und Strafzahlungen, Vertrauensverlust bei Kunden).

Vor diesem Hintergrund rücken regulatorische Vorgaben zur IT-Sicherheit in den Fokus der Präventionsstrategien. Die EU hat mit der zweiten Richtlinie zur Netz- und Informationssicherheit (NIS2)[2] einen neuen Rechtsrahmen geschaffen, der ein hohes Maß an Cybersicherheit in essenziellen und wichtigen Sektoren sicherstellen soll. NIS2 verpflichtet Unternehmen zu umfangreichen präventiven Sicherheitsmaßnahmen und bezieht erstmals die Geschäftsleitung ausdrücklich in die Verantwortung mit ein.[3] Diese Regulierung zielt darauf ab, die Resilienz der Wirtschaft gegenüber Cyber-Gefahren zu erhöhen und so auch Insolvenzen infolge von Cyberangriffen vorzubeugen.[4]

Dieser Beitrag beleuchtet, wie Cyberrisiken insolvenzrelevant werden (2.), welche Schutzpflichten NIS2 vorsieht (3.) und inwiefern deren Umsetzung geeignet ist, Insolvenzen zu verhindern (4.). Ein Fazit schließt die Untersuchung (5.).

2. Cyberrisiken als zunehmender Insolvenzauslöser

Cyberangriffe haben sich in den letzten Jahren von einem reinen IT-Problem zu einem potenziellen Existenzrisiko für Unternehmen entwickelt. Empirische Daten belegen die wachsende Brisanz: Laut Bitkom erlitten deutsche Unternehmen 2024 mit 266,6 Mrd. € den höchsten jemals gemessenen Jahresschaden durch Diebstahl digitaler Informationen, Spionage und IT-Sabotage. Vor allem Ransomware-Angriffe mit Verschlüsselung von Unternehmensdaten und anschließender Erpressung haben stark zugenommen und führen zu erheblichen Betriebsunterbrechungen. So berichten inzwischen rund 23 % der Firmen von erlittenen Ransomware-Schäden (Vorjahr: 12 %).[5] Die subjektive Bedrohungswahrnehmung hat sich entsprechend gedreht: Zwei Drittel der Unternehmen fühlen sich durch Cyberattacken existenziell bedroht.[6] Noch vor zwei Jahren nahm nur eine kleine Minderheit dieses Risiko so ernst, heute ist es mehrheitlicher Konsens in der Wirtschaft.

Die Realität liefert zahlreiche Praxisfälle, in denen Cybervorfälle zum dominierenden Insolvenzgrund wurden. Der eingangs erwähnte Fall *Fasana GmbH* ist besonders eindrücklich: Im Mai 2025 legten Hacker mittels Ransomware die gesamte IT eines mittelständischen Papierwarenherstellers lahm. Zwei Wochen lang stand die Produktion komplett still; Angebote konnten nicht bearbeitet, Rechnungen nicht gestellt werden. Der Umsatzausfall betrug mehrere Millionen Euro. Mangels liquider Mittel sah sich die Geschäftsführung am 1. Juni 2025 gezwungen, Insolvenzantrag zu stellen.[7] 240 Arbeitsplätze standen auf dem Spiel. Ähnlich erging es der *Schumag AG* in Aachen: Dieses Traditionsunternehmen (gegr. 1830, ca. 450 Mitarbeiter) war bereits angeschlagen und in einem Sanierungsprozess, als im September 2024 ein Hackerangriff die Lage eskalieren ließ. Der Angriff führte zu unerwarteten Produktionsausfällen, Verzögerungen von Zahlungseingängen und zusätzlichen Kosten, wodurch geplante Turnaround-Maßnahmen obsolet wurden. Die dadurch gerissenen Liquiditätslücken konnte das Unternehmen kurzfristig nicht schließen. *Schumag* musste Insolvenzantrag stellen, befindet sich aber im Rahmen eines Insolvenzverfahrens in Eigenverwaltung weiterhin im operativen Geschäft.[8] Weitere Beispiele werden bekannt: etwa die *Eu-Rec GmbH* (Recyclingunternehmen), die im Herbst 2024 nach einem Cyberangriff Insolvenzantrag stellte[9], oder diverse kommunale IT-Dienstleister, deren Leistungen nach Attacken ausfielen und nur durch

[1] WDR.de: Schumag meldet Insolvenz an; Aachener-Zeitung.de: Aachener Traditionsunternehmen Schumag ist gerettet; Merkur.de: Hackerangriff zwingt Traditionsfirma in die Knie: Insolvenz folgt

[2] ABI. EU L 333/80 v. 27.12.2022 (Richtlinie (EU) 2022/2555).

[3] Richtlinie (EU) 2022/2555, Art. 20 Abs. 2

[4] Richtlinie (EU) 2022/2555, Art. 21 f.

[5] Unternehmen Cybersicherheit, Bitkom-Studie: 52 Prozent der Unternehmen fühlen sich durch Cyberattacken in ihrer Existenz bedroht

[6] Bitkom, Angriffe auf die deutsche Wirtschaft nehmen zu

[7] FOCUS online: Wie ein Hackerangriff ein deutsches Traditionsunternehmen in die Insolvenz trieb; Stern.de: Erpresserbrief im Drucker: Hacker treiben Servietten-Fabrik in die Insolvenz

[8] Aachener-Zeitung.de: Aachener Traditionsunternehmen Schumag ist gerettet; Merkur.de: Verschlimmerte Lage durch Cyberattacke: Traditionsunternehmen mit über 400 Beschäftigten ist insolvent; FR.de: Cyberangriff zwingt Elektronikversicherer in die Knie

[9] Merkur.de: Familienunternehmen meldet nach Hackerangriff Insolvenz an

staatliche Nothilfen Schlimmeres verhindert werden konnte (Stichwort Doppik-Ausfall in Schwerin 2020 etc., hier nur illustrativ).[1]

Diese Fälle zeigen, dass unzureichende Cybersicherheit mittlerweile eine unmittelbare Gefahr für die Unternehmensfortführung darstellt. Besonders heimtückisch ist, dass Cyberangriffe meist überraschend und mit hoher Schlagkraft auftreten – betroffene Unternehmen verlieren in kurzer Zeit ihre operativen Fähigkeiten (z.B. durch Verschlüsselung aller Daten oder Zerstörung von Serversystemen). Ohne wirksamen Notfallplan können schon wenige Tage Ausfall genügen, um kritische Zahlungsengpässe herbeizuführen. Hinzu kommen Folgeschäden wie Vertragsstrafen wegen Lieferverzugs, Schadenersatzansprüche von Kunden (insb. bei Datenlecks gemäß DSGVO), Bußgelder der Behörden, teure IT-Forensik und Wiederherstellungsmaßnahmen, Reputationsverlust und damit einhergehende Umsatzrückgänge. Besonders für mittelständische Unternehmen ohne große Kapitalreserven kann ein gravierender Cybervorfall so schnell zur insolvenzrechtlichen Krise eskalieren.

Insolvenzrechtlich relevant ist ferner, dass Geschäftsleiter nach einem schweren Cybervorfall zeitnah prüfen müssen, ob ein Insolvenzeröffnungsgrund (Zahlungsunfähigkeit[2] oder Überschuldung[3]) vorliegt. Die Pflicht zur Insolvenzantragstellung innerhalb kurzer Frist gem. § 15a InsO, bleibt auch in solchen Fällen bestehen.[4] Ein Geschäftsführer, der trotz lahmgelegter IT und absehbarer Zahlungsstockung zögert, in der Hoffnung auf baldige Wiederherstellung, läuft Gefahr der Insolvenzverschleppung gem. § 15a Abs. 4 InsO – eine Straftat und Haftungsfalle.[5] Die neue Risikolage durch Cyberangriffe verschärft somit auch die Anforderungen an das Krisenmanagement der Leitungsebene.

Die Politik und Aufsichtsbehörden haben diese Entwicklung erkannt. Auf EU-Ebene wurde mit der NIS2-Richtlinie ein Instrument geschaffen, das durch präventive Sicherheitsvorgaben solchen Extremszenarien entgegenwirken soll. Im Folgenden wird das NIS2-Regime näher analysiert und dessen Eignung als Insolvenzpräventionsmechanismus erörtert.

3. Präventive Schutzpflichten des NIS2-Regimes für Unternehmen und Leitungsorgane

Die Richtlinie (EU) 2022/2555 (NIS2) verpflichtet eine Vielzahl von Unternehmen in der EU zu konkreten Cybersicherheitsmaßnahmen, um ein hohes gemeinsames Sicherheitsniveau zu erreichen. Sie löst die ältere NIS-Richtlinie von 2016 ab und erweitert sowohl den Anwendungsbereich als auch die Anforderungen deutlich. Anders als bislang beschränkt sich der Pflichtenkreis nicht mehr nur auf klassische KRITIS-Betreiber (kritische Infrastrukturen wie Energie, Wasser, Finanzen etc.), sondern umfasst nun auch zahlreiche weitere Sektoren und mittlere sowie größere Unternehmen („wesentliche“ und „wichtige“ Einrichtungen)[6]. So zählen z.B. Hersteller von Vorprodukten, Anbieter digitaler Dienste (Cloud, Rechenzentren, Online-Plattformen) und Teile des Mittelstands über gewissen Größenkriterien künftig dazu.[7] Kleinst- und Kleinunternehmen (weniger als 50 Mitarbeiter, weniger als 10 Mio. € Umsatz)[8] sind zwar im Regelfall ausgenommen, doch dehnt NIS2 den Kreis der Verpflichteten in die Breite der Wirtschaft aus – fast jedes größere Unternehmen kann betroffen sein. Unternehmen müssen daher eigenständig prüfen, ob sie unter den Anwendungsbereich fallen, etwa anhand ihres Sektors und finanzieller Schwellenwerte. National bieten Behörden wie das BSI hierfür Orientierungshilfen an (z.B. der NIS2-Betroffenheitscheck).[9]

Inhaltlich etabliert die NIS2-Richtlinie umfangreiche präventive Cybersicherheitspflichten. Im Kern verlangt Art. 21 NIS2 von allen betroffenen Unternehmen, „angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen“ zu ergreifen, um die Risiken für die

[1] Schwerin.de: Schweriner Stadtverwaltung von Schadsoftware betroffen; NDR.de: Erste Konsequenzen nach Hackerangriff auf Polizeihandys in MV
[2] *Noack/Servatius/Haas/Haas*, 24. Aufl. 2025, InsO § 17; B*raun/Salm-Hoogstraeten*, 10. Aufl. 2024, InsO § 17
[3] *Braun/Salm-Hoogstraeten*, 10. Aufl. 2024, InsO § 19; MüKoInsO/*Schüler*, 5. Aufl. 2025, InsO § 19
[4] MüKoInsO/*Klöhn*, 5. Aufl. 2025, InsO § 15a; *K. Schmidt* InsO/*K.Schmidt/Herchen*, 20. Aufl. 2023, InsO § 15a Rn. 31, 32; *Braun/Erbe*, 10. Aufl. 2024, InsO § 15a Rn. 16-18
[5] *Andres/Leithaus/Leithaus*, 5. Aufl. 2025, InsO § 15a Rn. 12, 13; BeckOK InsR/*Wolfer*, 39. Ed. 1.5.2025, InsO § 15a Rn. 30-36
[6] Richtlinie (EU) 2022/2555, Art. 3 i. V. m. Anhang I u. II
[7] Richtlinie (EU) 2022/2555 Anhang I Ziff. 8
[8] Richtlinie (EU) 2022/2555 i. V. m. RL (EU) 2016/1148 (ABl. L 124 vom 20.5.2003, S. 36-41)
[9] BSI: NIS-2 - Was tun?

Sicherheit der Netz- und Informationssysteme zu managen und die Auswirkungen von Sicherheitsvorfällen zu minimieren.[1] Diese Maßnahmen müssen den Stand der Technik berücksichtigen, an der individuellen Gefährdungslage des Unternehmens ausgerichtet sein und laufend angepasst werden. NIS2 konkretisiert erstmals einen Mindestkatalog von Sicherheitsmaßnahmen, der gem. Art. 21 Abs. 2 NIS2 zumindest umzusetzen ist. Dazu zählen insbesondere:

- Risikomanagement und IT-Sicherheitskonzepte: Verfahren zur systematischen Risikoanalyse sowie Policies zur Informationssicherheit. Hierunter fallen z.B. Vorgaben zur regelmäßigen Bewertung von Bedrohungen und Schwachstellen im Unternehmen.
- Vorfall-Management (Incident Response): Prozesse zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen. Jedes Unternehmen muss fähig sein, im Ernstfall schnell zu reagieren – etwa durch definierte Incident-Response-Teams, Meldungen an Behörden und interne Eskalationspläne.
- Betriebs- und Notfallkontinuität: Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs im Krisenfall, insbesondere Backup-Management, Disaster-Recovery-Pläne und Krisenmanagement-Strukturen. Konkret sind regelmäßige Datensicherungen zu erstellen, Ausfallpläne (Business Continuity Plans) zu entwickeln und Notfallübungen durchzuführen, um einen längerfristigen Betriebsstillstand zu verhindern.
- Sicherheit in der Lieferkette: Anforderungen an die Cybersecurity der Zulieferer und Dienstleister. Unternehmen müssen die Sicherheit ihrer unmittelbaren Lieferanten beurteilen (z.B. durch Auditierungen, vertragliche Sicherheitsklauseln) und Risiken durch Dritte in ihre Schutzkonzepte einbeziehen. Besonders kritische Lieferketten sollen EU-weit koordiniert bewertet werden.
- Sichere Entwicklung und Schwachstellen-Management: Vorgaben zur IT-Sicherheit bei Erwerb, Entwicklung und Wartung von Systemen sowie zum Umgang mit Schwachstellen (Vulnerability-Management). Dies umfasst u.a. sichere Programmierstandards, regelmäßige Updates/Patches und Verfahren zur Meldung und Behebung neu entdeckter Sicherheitslücken.
- Wirksamkeitsprüfungen: Verfahren, um die Effektivität der Cybersicherheitsmaßnahmen zu evaluieren. Beispiele sind interne oder externe Security Audits, Penetration-Tests oder Zertifizierungen. Dadurch soll sichergestellt werden, dass die implementierten Schutzmaßnahmen tatsächlich greifen.
- Basale Cyberhygiene und Schulung: Einführung grundlegender Sicherheitspraktiken im Alltag (z.B. Passwort-Richtlinien, regelmäßige Updates, Prinzip der minimalen Rechte) sowie regelmäßige Awareness-Schulungen der Mitarbeiter.[1] Menschliches Fehlverhalten (Phishing-Klicks, unsichere Passwörter) zählt zu den Hauptursachen erfolgreicher Angriffe; dem wirkt NIS2 durch Schulungspflichten entgegen.
- Kryptographie und Verschlüsselung: Vorgaben zur Anwendung von Kryptographie (z.B. Verschlüsselung sensibler Daten, Einsatz von VPN, elektronischen Signaturen) entsprechend dem Stand der Technik.
- Personalsicherheit und Zugangsmanagement: Maßnahmen zur Kontrolle von Zugriffsrechten, zur sicheren Identifizierung (z.B. Mehrfaktor-Authentifizierung) und zum Asset-Management.[1] Ziel ist es, Unbefugten den Zugriff zu verwehren und Missbrauch durch Insider zu verhindern. Auch Aspekte wie Zuverlässigkeitsüberprüfungen von IT-Administratoren oder Offboarding-Prozesse fallen darunter.
- Gesicherte Kommunikation und Notfallsysteme: Einsatz von sicheren Kommunikationsmitteln (verschlüsselte Sprach-, Video- und Textkommunikation) und Absicherung von Notfallkommunikationswegen[1], damit im Krisenfall die interne und externe Kommunikation funktioniert.

Diese breite Palette an Maßnahmen zeigt, dass NIS2 einen ganzheitlichen Sicherheitsansatz verfolgt. Technische Vorkehrungen (etwa Firewalls, Zugangskontrollen) greifen nur im Zusammenspiel mit organisatorischen Regelungen (Policies, Zuständigkeiten) und menschlichem Verhalten

[1] ABl. EU L 333/80 v. 27.12.2022, Art. 21

(Sensibilisierung, Training). Art. 21 Abs. 2 NIS2 verlangt ausdrücklich einen „gefahrenübergreifenden Ansatz“, der sowohl Cyber- als auch physische Risiken umfasst und auf Prävention, Detektion, Reaktion sowie Wiederherstellung abzielt.[1] Damit wird Resilienz zum Leitmotiv: Unternehmen sollen Angriffe nicht nur verhindern, sondern auch ihre Auswirkungen begrenzen und möglichst schnell wieder funktionsfähig werden.

Neben den präventiven Anforderungen statuiert NIS2 auch Meldepflichten gem. Art. 23 NIS2 bei Sicherheitsvorfällen. Bedeutsame Zwischenfälle müssen unverzüglich (binnen 24 Stunden erste Meldung, binnen 72 Stunden eine Aktualisierung und Abschlussbericht nach spätestens einem Monat) an die zuständige Behörde bzw. das Computer-Notfallteam (CSIRT) gemeldet werden.[2] Diese Pflicht zur Incident-Notification soll einerseits Behörden ermöglichen, Frühwarnungen zu geben und koordinierte Gegenmaßnahmen einzuleiten, andererseits erhöht sie den Druck auf Unternehmen, Transparenz über ihre Sicherheitsvorfälle herzustellen. Verschweigen oder verspätetes Melden eines Cybervorfalls kann als Verstoß geahndet werden.[3] Für die hiesige Thematik (Insolvenzprävention) ist die Meldepflicht mittelbar relevant: Sie verbessert den Informationsfluss und kann im Krisenfall Unterstützung aktivieren (z.B. Hilfestellung durch Behörden/BSI bei der Bewältigung eines großflächigen Angriffs). Zudem zwingt sie Unternehmen dazu, Incident-Response-Prozesse einzurichten – was wiederum Teil einer guten Krisenbewältigung ist.

Ein zentrales Novum der NIS2-Richtlinie ist die ausdrückliche Einbindung der Geschäftsleitungen der betroffenen Unternehmen in die Cybersicherheits-Verantwortung. Art. 20 NIS2 („Governance“) verpflichtet die Leitungsorgane wesentlicher und wichtiger Einrichtungen (also Vorstände, Geschäftsführungen etc.), die nach Art. 21 erforderlichen Sicherheitsmaßnahmen persönlich zu billigen und ihre Umsetzung zu überwachen. Die Mitgliedstaaten müssen sicherstellen, dass Geschäftsleiter für Verstöße des Unternehmens gegen diese Pflichten auch haftbar gemacht werden können. Konkret bedeutet dies, dass sich die oberste Führungsebene sich aktiv mit dem Cybersicherheits-Risikomanagement auseinandersetzen muss, z.B. durch Beschlussfassung über die IT-Sicherheitsstrategie, regelmäßige Lageberichte des CISO etc. Ein bloßes Delegieren an die IT-Abteilung genügt nicht; das Top-Management trägt letztverantwortlich die Kontrolle. Außerdem schreibt Art. 20 Abs. 2 NIS2 vor, dass die Mitglieder der Leitungsorgane regelmäßig an Schulungen teilnehmen müssen, um ausreichende Kenntnisse und Fähigkeiten im Bereich Cybersecurity-Risikomanagement zu erlangen.[4] Dies soll verhindern, dass Unwissen oder fehlendes Problembewusstsein auf Vorstandsebene zu Nachlässigkeit führt – jeder Geschäftsführer muss ein Grundverständnis für Cyberrisiken und Schutzkonzepte entwickeln.

Mit diesen Vorgaben etabliert NIS2 einen Sorgfaltsmaßstab für die Unternehmensleitung in Sachen IT-Sicherheit. Geschäftsleiter müssen organisatorisch sicherstellen, dass ihr Unternehmen die vorgeschriebenen Sicherheitsvorkehrungen umsetzt. Tun sie dies nicht, drohen einerseits aufsichtsrechtliche Konsequenzen (dazu sogleich

[1] ABl. EU L 333/80 v. 27.12.2022, Art. 21
[2] ABl. EU L 333/80 v. 27.12.2022, Art. 23
[3] ABl. EU L 333/80 v. 27.12.2022, Art. 32
[4] ABl. EU L 333/80 v. 27.12.2022, Art. 20 Abs. 2

unter Punkt 4), andererseits bergen Vernachlässigungen auch zivilrechtliche Haftungsrisiken. Die Richtlinie betont, dass Cybersicherheit Teil der Corporate Governance und Compliance des Unternehmens ist. Entsprechend wurde in den deutschen Umsetzungsgesetz-Entwurf (RegE NIS2UmsuCG), der von der Bundesregierung beschlossen, aber vom Deutschen Bundestag noch nicht verabschiedet wurde, eine Norm (§ 38 BSIG-E) aufgenommen, die das persönliche Haftungsrisiko der Leitung noch unterstreicht.[1]

Zusammengefasst errichtet das NIS2-Regime ein engmaschiges Netz von Präventionspflichten: Unternehmen müssen umfassende technische und organisatorische Sicherheitsmaßnahmen etablieren, ihre Lieferbeziehungen absichern, Notfallpläne bereithalten, Vorfälle melden – und das Top-Management steht in der Pflicht, all dies aktiv voranzutreiben und zu verantworten. Diese Regulierung greift damit weit in die unternehmerische Praxis ein. Im nächsten Abschnitt wird erörtert, ob und wie diese Pflichten dazu beitragen können, Insolvenzen aufgrund von Cybervorfällen vorzubeugen.

4. NIS2-Umsetzung als Instrument der Insolvenzprävention

Die leitende Idee hinter NIS2 ist es, durch verbindliche Sicherheitsvorkehrungen die Wahrscheinlichkeit und Schwere von Cybervorfällen zu reduzieren, um dadurch auch gravierende wirtschaftliche Schäden und letztlich Insolvenzen abzuwenden. Im Erwägungsgrund der Richtlinie wird ausdrücklich darauf hingewiesen, dass die steigende Zahl und Wirkung von Cybervorfällen eine große Bedrohung für die wirtschaftlichen Aktivitäten im Binnenmarkt darstellt – Vorfälle können die Ausübung von Tätigkeiten beeinträchtigen, finanzielle Verluste verursachen und der Wirtschaft erheblichen Schaden zufügen. Prävention und Effektivität der Cybersicherheit seien daher von zentraler Bedeutung, um die Vorteile der Digitalisierung gefahrlos nutzen zu können.[2] Mit NIS2 will der Gesetzgeber also einen präventiven Schutzschirm aufspannen, der Unternehmen robuster gegen Angriffe macht und so katastrophale Folgen wie Betriebsausfälle und Insolvenzen möglichst verhindert.

Im Einzelnen lassen sich mehrere Mechanismen identifizieren, durch die die NIS2-Maßnahmen insolvenzpräventiv wirken:

(a) Risikoreduzierung und Schadensbegrenzung

Die geforderten Sicherheitsmaßnahmen – insbesondere im Bereich Incident Response, Business Continuity und Disaster Recovery – zielen darauf ab, die Ausfallszeiten und Schadensausmaße im Falle eines Angriffs zu minimieren. Zentral ist hierbei die Pflicht zu Backups und Notfallplänen.[3] Verfügt ein Unternehmen über aktuelle, offline gesicherte Datenbackups und erprobte Wiederanlaufpläne, kann ein Ransomware-Angriff weit schneller behoben werden, oft ohne Lösegeldzahlung. Die Produktion kann – zumindest teilweise – wieder anlaufen, Lieferverpflichtungen können nach kurzer Verzögerung erfüllt werden. So lässt sich der Umsatzausfall begrenzen, der im worst case zur Zahlungsunfähigkeit führen würde. Ein Beispiel: Hätte *Fasana* über ein robustes Offline-Backup-System und ein eingeübtes Notfallkonzept verfügt, wären die Systeme womöglich binnen Tagen wiederherstellbar gewesen, anstatt zwei Wochen handlungsunfähig zu sein. NIS2 macht solche Vorkehrungen nun verpflichtend. Insolvenzrechtlich kann dies den Unterschied ausmachen, ob nach einem Angriff noch ausreichend Liquidität vorhanden ist, um den Betrieb aufrechtzuerhalten, oder ob ein Insolvenzantrag gestellt werden muss.

(b) Vermeidung von Sorgfaltspflichtverletzungen und Folgeschäden

Viele der gravierendsten Schäden nach Cybervorfällen entstehen durch Folgeansprüche – z.B. Datenschutzstrafen, Schadenersatzklagen von Kunden oder Vertragsstrafen wegen nicht erfüllter Aufträge. Wenn ein Unternehmen nachweisen kann, angemessene Sicherheitsmaßnahmen getroffen zu haben, lassen sich solche Ansprüche ggf. abmildern. So sehen Datenschutzbehörden bei DSGVO-Verstößen (z.B. Datenleck) das Ausmaß der technischen Schutzmaßnahmen als Kriterium

[1] NIS2UmsuCG (Gesetzentwurf v. 25.07.2025)
[2] ABl. EU L 333/80 v. 27.12.2022, Rn. 3
[3] ABl. EU L 333/80 v. 27.12.2022, Art. 21

für Bußgelder an.[1] Ein NIS2-konformes Unternehmen hat zumindest eine Verteidigungslinie und kann darlegen, alle vorgeschriebenen Vorkehrungen getroffen zu haben (Stand der Technik), was etwa bei Gerichtsverfahren als Entlastung dienen könnte. Umgekehrt führt Nichtbeachtung elementarer Sicherheitsstandards häufig zu einer Verschärfung der Haftung – Gerichte könnten grobe Fahrlässigkeit der Geschäftsführung annehmen, was Ansprüche begünstigt. Durch NIS2 werden diese Standards nun klar umrissen, was die Rechtsposition vorsorglicher Unternehmen stärkt. Indirekt dient dies der Insolvenzprävention: Wer Haftungs- und Bußgeldrisiken senkt, schont sein Kapital.

(c) Etablierung einer Sicherheitskultur und Früherkennung

NIS2 fordert laufendes Risikomanagement und Einbindung der Leitung, was die Awareness im ganzen Unternehmen steigert. Cybersecurity wird Chefsache.[2] Dieses erhöhte Bewusstsein kann dazu führen, dass Warnsignale früher erkannt und behoben werden, bevor ein größerer Schaden entsteht. Beispielsweise werden Unternehmen Schwachstellen-Reports (z.B. vom BSI oder externen Stellen) ernster nehmen und proaktiv patchen, um gar nicht erst Opfer zu werden. Die Früherkennung von Risiken deckt sich mit insolvenzpräventiven Grundsätzen im deutschen Recht (§ 1 StaRUG, dazu unten). Mit anderen Worten: NIS2-Compliance fördert eine proaktive Sicherheitshaltung, die extreme Krisenfälle verhindern kann, bevor sie entstehen.

(d) Vermeidung von Kettenreaktionen in Lieferketten

Ein besonderes Risiko für Insolvenzen sind Lieferkettenausfälle – wenn ein Zulieferer cyberbedingt ausfällt, kann das nachgelagerte Hersteller in die Knie zwingen (Produktionsstopp, Konventionalstrafen). NIS2 adressiert das durch Pflichten zur Lieferketten-Sicherheit und -Kontrolle.[3] Große Unternehmen werden verstärkt prüfen, ob ihre kleineren Partner ausreichende Sicherheit vorweisen. Dies wirkt druckvoll auf die gesamte Wertschöpfungskette, da auch nicht direkt regulierte Zulieferer aufrüsten müssen, um im Geschäft zu bleiben (ansonsten droht Ausschluss von Aufträgen).[4] Dadurch reduziert sich das Risiko, dass ein einzelnes schwaches Glied die ganze Kette gefährdet. Aus insolvenzrechtlicher Sicht wird die Gefahr dominoartiger Insolvenzen (Zulieferer bricht weg, Hersteller gerät in Schieflage) verringert.

(e) Externe Unterstützung und Informationsaustausch

Durch das Melde- und Kooperationssystem von NIS2 (CSIRTs, EU-CyCLONe) kann im Großschadensfall rascher externe Unterstützung mobilisiert werden. Beispielsweise kann das nationale Computer-Notfallteam bei einem branchenweiten Angriff koordinierend helfen, Warnungen frühzeitig an andere senden und damit Schadenbegrenzung betreiben. Zwar richtet sich dies primär an die öffentliche Sicherheit, doch

[1] *Kühling/Buchner/Schröder*, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 20 Rn. 1-3, Art. 84 Rn. 14, 15

[2] *Degen/Emmert Elektron*, Rechtsverkehr, 3. Aufl. 2025, § 11 Rn. 13

[3] ABI. EU L 333/80 v. 27.12.2022, Art. 14, 22

[4] ABI. EU L 333/80 v. 27.12.2022, Art. 21 Abs. 3, Art. 22

indirekt profitieren auch einzelne Unternehmen, weil sie nicht mehr isoliert einer Cyberkrise begegnen müssen. Im Idealfall kann so eine Krise gemeistert werden, ohne dass betroffene Unternehmen Insolvenz anmelden müssen.

Angesichts dieser Punkte scheint das NIS2-Regime einen wichtigen Beitrag zur Insolvenzprävention zu leisten. Resilienz – also die Fähigkeit, trotz Angriff handlungsfähig zu bleiben – ist der Schlüssel, um existenzbedrohende Lagen abzuwenden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont entsprechend die Bedeutung einer resilienten Cybersicherheitsarchitektur als Voraussetzung für die Bestandssicherung von Unternehmen.[1] Die NIS2-Pflichten zielen darauf ab, genau diese Resilienz aufzubauen.

Allerdings darf man die Wirkung nicht überschätzen da es absolute Sicherheit nicht gibt. Selbst NIS2-konforme Unternehmen können Opfer neuartiger, hochkomplexer Angriffe werden, die bestehende Schutzmechanismen überwinden. NIS2 mindert Risiken, eliminiert sie aber nicht vollständig. Entscheidend ist die praktische Umsetzung, denn nur wenn die vorgeschriebenen Maßnahmen auch tatsächlich und gewissenhaft implementiert werden und nicht bloß auf dem Papier existieren, entfalten sie ihre Schutzwirkung. Unternehmen müssen also real investieren – in sichere IT-Architekturen, in qualifiziertes Personal, in regelmäßige Tests. Der Erfolgsdruck ist hoch, da die Nichteinhaltung nun auch sanktioniert wird (siehe Abschnitt 4).

Zu beachten ist ferner, dass NIS2 nur für bestimmte Unternehmen gilt. Kleine Unternehmen außerhalb kritischer Sektoren werden nicht direkt erfasst. Gerade diese sind aber oft besonders schutzbedürftig, da ihnen Ressourcen und Expertise für IT-Sicherheit fehlen. Hier bleibt eine Regulierungslücke, denn ein Cyberangriff auf ein kleines Familienunternehmen kann ebenso zur Insolvenz führen, doch greift NIS2 dort nicht zwingend. Die Richtlinie verweist lediglich darauf, dass die Mitgliedstaaten die besonderen Bedürfnisse von KMU in ihren Strategien berücksichtigen sollen.[2] In der Praxis wird diese Flanke teilweise durch Marktmechanismen geschlossen (z.B. fordern große Auftraggeber Sicherheitsnachweise auch von kleineren Zulieferern; Versicherer setzen Mindeststandards voraus). Dennoch bleibt fraglich, ob ohne direkte Verpflichtung die Präventionskultur in der gesamten Breite der Wirtschaft ankommt. Hier könnten nationale Initiativen (Förderprogramme für KMU-Cybersicherheit, branchenspezifische Standards) ergänzend nötig sein, um Insolvenzen in diesem Segment vorzubeugen.

Zusammenfassend bietet NIS2 den Rahmen für eine deutlich verbesserte Krisenvorsorge gegen Cyberrisiken. Werden die Vorgaben konsequent umgesetzt, ist zu erwarten, dass Unternehmen Angriffe besser überstehen und weniger häufig in existenzielle Nöte geraten. Die Prämisse lautet: Schützen statt Sanieren – durch präventive Sicherheitspflichten Insolvenzen gar nicht erst entstehen zu lassen. Im nächsten Abschnitt wird betrachtet, welche rechtlichen Konsequenzen drohen, wenn Unternehmen oder ihre Leitungsorgane diese Pflichten vernachlässigen, und wie dies mit bestehenden insolvenzrechtlichen Verantwortlichkeiten zusammenhängt.

5. Fazit

Cyberangriffe sind ein wesentlicher Insolvenzauslöser moderner Unternehmenskrisen. Die NIS2-Richtlinie setzt mit verbindlichen Pflichten für technische, organisatorische und personelle Schutzmaßnahmen einen neuen Präventionsrahmen, der auch insolvenzrechtlich von erheblicher Bedeutung ist. Durch Backups, Notfallpläne, Incident-Response-Strukturen und die Einbindung der Geschäftsleitung in die Verantwortung wird die Resilienz gegen Angriffe gestärkt und die Wahrscheinlichkeit insolvenzbedrohender Krisen reduziert. Gleichwohl bleiben Grenzen: Kleinunternehmen werden nicht vollständig erfasst, absolute Sicherheit ist nicht erreichbar, und die Wirksamkeit hängt von konsequenter Umsetzung ab. Insgesamt etabliert NIS2 jedoch ein robustes Schutzinstrument, das Insolvenzen durch Cyberangriffe zwar nicht vollständig ausschließt, aber deutlich unwahrscheinlicher macht.

[1] BSI: DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2024; BSI: Mindeststandards Bund

[2] Richtlinie (EU) 2022/2555, Art. 7 Abs. 1