VEREINIGUNG
DER HESSISCHEN
UNTERNEHMERVERBÄNDE

Arbeitsrecht

Die rechtliche Dimension von Cyberattacken – was Unternehmen präventiv und im Ernstfall rechtlich tun sollten

Ein Leitfaden für Mitglieder

Impressum

Autoren:

Rechtsanwalt Dr. Oliver Hornung
SKW Schwarz Rechtsanwälte
T +49 69 630001-65
o.hornung@skwschwarz.de

Bearbeitet von:

Rechtsanwalt Prof. Dr. Franz-Josef Rose
HESSENMETALL
Leiter der Rechtsabteilung
Fachanwalt für Arbeitsrecht
Frankfurt am Main
T +49 69 95808-170
F +49 69 95808-126
frose@hessenmetall.de

Herausgeber:

HESSENMETALL
Verband der Metall- und Elektro-Unternehmen Hessen e. V.
Emil-von-Behring-Straße 4, 60439 Frankfurt am Main
T +49 69 95808-0
F +49 69 95808-126
info@hessenmetall.de
www.hessenmetall.de

Dieser Leitfaden ist mit großer Sorgfalt erstellt worden. Er ersetzt gleichwohl die Beratung im Einzelfall nicht. Mit der Bitte um Verständnis wird darauf hingewiesen, dass keinerlei Haftung übernommen wird. Alle Angaben dieser Publikation beziehen sich grundsätzlich auf alle Geschlechter. Aus Gründen der einfacheren Sprache und ohne jede Diskriminierungsabsicht wurde auf eine Bezeichnung mit dem Genderstern * verzichtet.

Vorwort

Die gesamte deutsche Wirtschaft und damit auch die hessischen Unternehmen stehen derzeit vor großen Herausforderungen. Nicht nur die Energieversorgung, auch die weltweiten Lieferketten sind in Gefahr. Hinzu kommen Angriffe, die die Hard- und Software eines Unternehmens betreffen können, Cyberattacken genannt. Die Gefahr, dass das Vertrauen von Kunden und Lieferanten verloren geht, ist groß.

In einer Welt, die immer vernetzter und digitaler wird, ist die Sicherheit von IT-Systemen nicht nur eine technische, sondern auch eine unternehmerische Notwendigkeit. Ein effektives Sicherheitskonzept kann entscheidend dazu beitragen, wirtschaftliche Verluste und Reputationsschäden zu vermeiden. Daher ist es unerlässlich, dass Unternehmen proaktive Maßnahmen ergreifen, um sich gegen die vielfältigen Bedrohungen zu wappnen.

Der folgende Leitfaden soll sowohl präventiv als auch in der rechtlichen Abwehr den hessischen Unternehmen helfen, Cyberattacken vorzubeugen. Der Leitfaden ist von SKW Schwarz Rechtsanwälte für HESSENMETALL erstellt worden und wurde der VhU zur Verfügung gestellt, dafür bedanken wir uns sehr herzlich.

Dirk Pollert Prof. Dr. Franz-Josef Rose

Januar 2025

Inhaltsverzeichnis

1. Einleitung – Worum geht's?

1.1 Ziel des Leitfadens

Die Wirtschaft steht mehr denn je im Fokus von Cyberbedrohungen. Cybervorfälle wie Datenlecks, Ransomware-Angriffe oder gezielte Phishing-Attacken können nicht nur immense finanzielle Schäden verursachen, sondern auch das Vertrauen von Kunden und Geschäftspartnern nachhaltig beeinträchtigen. Es gehört zur **unternehmerischen Sorgfaltspflicht**, diesem Szenario durch das Treffen entsprechender Vorkehrungen vorzubauen. Nachlässigkeiten und der Verstoß gegen Sorgfaltspflichten kosten das Unternehmen Geld und Vertrauen. In vielen Fällen können sie Haftungstatbestände auslösen, sei es gesetzlicher, sei es vertraglicher Art.

Es ist zu beobachten, dass sich Unternehmen des rechtlichen (und damit auch wirtschaftlichen) Ausmaßes eines Cybervorfalles oftmals erst dann gewahr werden, wenn der Ernstfall eintritt. Die Erfahrung zeigt außerdem, dass die Unternehmen, die sich mit dem Thema professionell beschäftigen und einen „Plan" entwickelt haben - und zwar sowohl für den präventiven Schutz als auch für die Ergreifung repressiver Sofortmaßnahmen im Ernstfall - deutlich stabiler in einer Cyberkrise agieren können als andere Unternehmen.

Dieser Leitfaden soll Unternehmen dabei unterstützen, sowohl **präventive** Maßnahmen zu ergreifen, als auch **im Ernstfall** richtig zu handeln.

Bestandteil des Leitfadens sind auch **mehrere Checklisten,** in denen die im Leitfaden angesprochenen Aspekte enthalten sind (z. B. eine Checkliste für die rechtlich gebotenen Sofortmaßnahmen im Falle eines Cybervorfalles, Anhang 4).

1.2 Rechtliche Relevanz von Cybervorfällen

Die Verletzung unternehmerischer Sorgfaltspflichten in Bezug auf Cyber-Risikomanagementmaßnahmen kann unterschiedliche Haftungs- und Schadensersatztatbestände auslösen. Im Zusammenhang mit Cybervorfällen liegt zudem der reflexartige Gedanke an das Datenschutzrecht nahe. Zwar muss das Datenschutzrecht im Fokus stehen, aber darüber hinaus können Cybervorfälle in einigen weiteren Bereichen rechtliche Implikationen haben, wie die nachfolgende Aufstellung zeigt.

Datenschutzrecht

Bei einem Cybervorfall, der personenbezogene Daten betrifft, greifen die Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Unternehmen müssen unter bestimmten Voraussetzungen Datenschutzverletzungen unverzüglich der zuständigen Aufsichtsbehörde melden und betroffene Personen informieren (s. u.). Verstöße hiergegen können zu erheblichen Bußgeldern und Schadensersatzansprüchen führen. Desgleichen gilt hinsichtlich unzureichender technischer und organisatorischer (präventiver) Maßnahmen, die ursächlich für den Cybervorfall waren.

IT-Sicherheitsrecht

Das IT-Sicherheitsrecht umfasst nationale und europäische Vorschriften wie das BSI-Gesetz, die KRITIS-Verordnung, die sehr bald geltende NIS-2 bzw. das deutsche Umsetzungsgesetz von NIS-2 (wird umgesetzt v. a. im BSI-Gesetz) sowie den voraussichtlich ab 2027 geltenden Cyber Resilience Act. Diese Gesetze verpflichten die betroffenen Unternehmen u. a., (i) prä-

ventiv angemessene Maßnahmen zur IT-Sicherheit und zum Cyberrisikomanagement zu implementieren und (ii) repressiv Sicherheitsvorfälle binnen bestimmter Fristen und nach einem abgestuften System an die zuständigen Sicherheitsbehörden zu melden.

Vertragsrecht und Haftung gegenüber Vertragspartnern

Cybervorfälle können die Erfüllung vertraglicher Pflichten beeinträchtigen und Haftungsfragen auslösen. Verträge mit Kunden, Lieferanten und Dienstleistern enthalten oft Bestimmungen zur IT-Sicherheit. Wenn diese Bestimmungen nicht eingehalten werden und dies infolge eines Cybervorfalles ursächlich für einen Schaden beim Vertragspartner ist (z. B. bedingt durch einen Lieferverzug), kann dies umfangreiche Schadensersatzforderungen des Vertragspartners (oder seiner Versicherung, die diesen Schaden im Innenverhältnis zunächst reguliert hat und nun beim betroffenen Unternehmen Regress nimmt) auslösen. Ein weiterer Aspekt ist der mögliche Betriebsausfall, der durch einen Cybervorfall verursacht wird. Wenn dadurch ebenfalls Lieferverpflichtungen in der Lieferkette nicht erfüllt werden können, kann dies ebenfalls zu schuldhaften Vertragsverletzungen und erheblichen Schadensersatzansprüchen führen.

Strafrecht

Hackerangriffe, Datenmanipulation oder Datendiebstahl sind strafbare Handlungen, die strafrechtliche Ermittlungen und Verfahren nach sich ziehen können. Unternehmen sollten in solchen Fällen eng mit den Strafverfolgungsbehörden zusammenarbeiten. Strafrechtliche Relevanz hat im Übrigen auch die Frage, ob Lösegeldforderungen von Hackern nachgekommen werden soll oder nicht. Die Zahlung von Lösegeld kann strafbar sein.

Sorgfaltspflichten und Haftung der Unternehmensführung

Die Unternehmensführung kann im Innenverhältnis gegenüber dem Unternehmen und im Außenverhältnis gegenüber einem Dritten für Cybervorfälle haftbar gemacht werden, wenn sie ihre Sorgfaltspflichten im Bereich der IT-Sicherheit verletzt hat und dies ursächlich für den Cybervorfall war.

Arbeitsrecht

Auch das Arbeitsrecht kann durch Cybervorfälle tangiert werden, etwa Regelungen zur Nutzung von IT-Systemen und Datenschutzpflichten der Mitarbeiter*innen. Unternehmen sollten klare Richtlinien und Schulungen zur IT-Sicherheit und zum Datenschutz implementieren. Letztlich ist dies wiederum Teil eines hinreichenden Cyber-Risikomanagements gemäß den Vorschriften des IT-Sicherheitsrechts sowie des Datenschutzrechts.

Presserecht

Wenn infolge eines Cybervorfalls negativ oder falsch über das Unternehmen berichtet wird oder ein potenzielles Fehlverhalten bzw. Versäumnis von Verantwortlichen oder einzelnen Mitarbeitern in den Raum gestellt wird, kann dies zu einer Rufschädigung des Unternehmens oder von einzelnen betroffenen Personen führen. Unternehmen müssen erwägen, ob und inwieweit sie hiergegen presserechtlich vorgehen möchten und/oder welche Kommunikationsstrategie sie grundsätzlich verfolgen möchten.

Die rechtlichen Implikationen von Cybervorfällen sind somit sehr vielfältig und betreffen zahlreiche Rechtsgebiete.

1.3 Fiktive Fallbeispiele

Um die Vielfältigkeit von Cybervorfällen und ihrer rechtlichen Implikationen zu verdeutlichen, seien nachfolgend drei fiktive Fallbeispiele genannt, auf die im Laufe des Leitfadens Bezug genommen werden.

Fallbeispiel 1: Metallverarbeitendes Unternehmen

Unternehmen: StahlTech GmbH

Vorfall: Die Produktionsanlagen der StahlTech GmbH werden durch einen gezielten Cyberangriff lahmgelegt. Hacker haben es geschafft, Schadsoftware in das industrielle Steuerungssystem (ICS) einzuschleusen, was zur Unterbrechung der Produktion führt. Dies verursacht erhebliche finanzielle Verluste und Verzögerungen in den Lieferketten. Parallel dazu berichtet die Presse über den Vorfall und erhebt den Verdacht, dass der Cyberangriff auf jahrelange Missachtung gängiger IT-Sicherheitsvorschriften und Normen durch die Geschäftsführung zurückzuführen ist. Es wird öffentlich der sofortige Rücktritt der Geschäftsleitung gefordert.

Fallbeispiel 2: Elektrogerätehersteller

Unternehmen: ElektroInnovate AG

Vorfall: Die ElektroInnovate AG stellt fest, dass Hacker in ihr Netzwerk eingedrungen sind und (i) vertrauliche Produktentwicklungsdaten sowie (ii) sämtliche Beschäftigtendaten (u. a. Gehälter) aus der eingesetzten HR-Software gestohlen haben. Die Produktentwicklungsdaten umfassen auch Patente und technische Spezifikationen für neue Elektrogeräte, die sich derzeit in der Entwicklung befinden, sowie Geschäftsgeheimnisse von Kooperationspartnern. Der Diebstahl könnte sowohl dem Unternehmen als auch den Kooperationspartnern einen erheblichen Wettbewerbsschaden zufügen.

Fallbeispiel 3: Hersteller von vernetzten Kühlschränken

Unternehmen: CoolTech GmbH

Vorfall: Ein Mitarbeiter der CoolTech GmbH, einem Hersteller von vernetzten Kühlschränken, fällt auf eine geschickt gestaltete Phishing-E-Mail herein. Durch die Eingabe seiner Zugangsdaten auf einer gefälschten Webseite erhalten die Angreifer Zugriff auf das interne Netzwerk des Unternehmens. Dort stehlen sie sensible Daten, einschließlich der Firmware und Sicherheitsprotokolle der vernetzten Kühlschränke. Zusätzlich manipulieren sie die Software-Updates, wodurch die Kühlschränke für Cyberangriffe anfällig werden. Die Hacker fordern ein Lösegeld in Kryptowährung, um die gestohlenen Daten nicht zu veröffentlichen und die Manipulation der Software-Updates rückgängig zu machen.

2. Regulatorischer Rahmen – Welche Vorschriften müssen Unternehmen im Kontext von Cybervorfällen beachten?

Der regulatorische Rahmen für den Umgang mit Cybervorfällen ist vielschichtig und umfasst eine Reihe von Gesetzen und Vorschriften, die Unternehmen einhalten müssen. Dieses Kapitel gibt einen Überblick über die wichtigsten gesetzlichen Anforderungen und deren praktische Relevanz.

2.1 IT-Sicherheitsgesetze (v. a. BSI-Gesetz, BSI-KritisV, NIS-2, Cyber Resilience Act)

IT-Sicherheitsgesetze bilden die Grundlage für die Sicherheitsarchitektur von Unternehmen und definieren spezifische Anforderungen und Meldepflichten.

Für Unternehmen der Metall- und Elektroindustrie sind vor allem die nachfolgend genannten Gesetze/Vorschriften praxisrelevant.

BSI-Gesetz und BSI-KritisV

- Betreiber Kritischer Infrastrukturen[1] sind verpflichtet, **angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme,** Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden.

- Betreiber Kritischer Infrastrukturen sind zudem verpflichtet, sogenannte Störungen, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der IT-Systeme geführt haben, oder erhebliche Störungen, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der IT-Systeme führen können, **unverzüglich an das BSI zu melden**.

NIS-2 Richtlinie und deutsches Umsetzungsgesetz[2]

- Die europäische NIS-2-Richtlinie (nachfolgend NIS-2) wurde Ende 2022 verabschiedet und ersetzt die Richtlinie zur Gewährleistung von Netzwerk- und Informationssicherheit (NIS-1) aus dem Jahr 2017.

- Der Zeitplan des deutschen Umsetzungsgesetzes sieht aktuell (Stand Oktober 2024) so aus, dass es im März 2025 in Kraft treten soll. Bis dahin gilt das BSI-Gesetz und die BSI-KritisV in seiner bzw. ihrer aktuellen Fassung (s. o.).

- Die Vorgaben von NIS-1 werden bislang v. a. durch das aktuell geltende BSI-Gesetz und die BSI-KritisV umgesetzt (s. o.). Adressiert werden bislang Betreiber kritischer Infrastrukturen (s. o.).

- Das wird sich künftig ändern. Denn der Anwendungsbereich von NIS-2 wird gegenüber NIS-1 **um einige Wirtschaftssektoren und Bereiche erweitert**. Unter anderem wird auch der Sektor „Verarbeitendes Gewerbe/Herstellung von Waren“ von NIS-2 bzw.

[1] Welche Unternehmen hierunter fallen, ist der BSI-KritisV zu entnehmen, https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

[2] NIS-2 wird künftig v.a. im dann aktualisierten und angepassten BSI-Gesetz umgesetzt

dem deutschen Umsetzungsgesetz umfasst. Welche Tätigkeiten und Unternehmen konkret hierunter fallen, ist den Anlagen 1 und 2 des deutschen Umsetzungsgesetzes im Einzelnen zu entnehmen.[3]

- Abgesehen von der Zugehörigkeit zu einem von NIS-2 erfassten Sektor fallen Unternehmen nur in den Anwendungsbereich von NIS-2 bzw. des deutschen Umsetzungsgesetzes, wenn sie zusätzlich die vorgesehenen Schwellenwerte erreichen. Dies ist (nur) der Fall, wenn sie (i) > 50 MA oder (ii) einen Jahresumsatz von mehr als EUR 10 Mio. und eine Jahresbilanzsumme von mehr als EUR 10 Mio. haben.

- Es werden künftig auch eine Vielzahl an **kleinen bis mittelständischen Unternehmen aus der Metall- und Elektroindustrie** vom (künftigen) BSI-Gesetz erfasst sein. Insoweit wird häufig der von NIS-2 erfasste Sektor „Verarbeitendes Gewerbe/Herstellung von Waren" einschlägig sein. Innerhalb dieses Sektors verweist Anlage 2 des deutschen Umsetzungsgesetzes auf die sogenannten NACE Rev. 2, eine europäische Verordnung zur Klassifizierung von Wirtschaftszweigen, und dort konkret auf die Liste im Abschnitt C Abteilungen 26 - 30.[4]

- Nach dieser Systematik fällt ein Unternehmen unter NIS-2 bzw. das deutsche Umsetzungsgesetz, wenn es Waren herstellt, die in einer der im Abschnitt C aufgeführten Abteilungen 26-30 der NACE Rev. 2 genannt sind. Um dies bestimmen zu können, ist eine exakte Bestimmung des Tätigkeitsbereiches des betroffenen Unternehmens von entscheidender Bedeutung.

- Übertragen auf die **Fallbeispiele 1 und 2** ist denkbar, dass die dort genannten Unternehmen StahlTech GmbH und ElektroInnovate AG unter den von NIS-2 bzw. dem deutschen Umsetzungsgesetz erfassten Sektor „Verarbeitendes Gewerbe/Herstellung von Waren" fallen (vgl. den Link in Fußnote 3). Für eine finale Prüfung der Betroffenheit unter NIS-2 hält der Sachverhalt jedoch keine ausreichenden Angaben bereit. Insbesondere lässt der Sachverhalt offen, welche konkreten Waren diese Unternehmen herstellen. In der Praxis muss geprüft werden, ob die Tätigkeitsbereiche des in Betracht kommenden Unternehmens unter eine der im Abschnitt C aufgeführten Abteilungen 26 - 30 der NACE Rev. 2 fallen.

- Unternehmen aus der **Metall- und Elektroindustrie** ist zu empfehlen, der Betroffenheitsanalyse unter NIS-2 eine besondere Beachtung zu schenken. Aufgrund der beschriebenen, feingliederigen Differenzierung in der NACE Rev. 2 kann es von Kleinigkeiten im konkreten Tätigkeitsbereich abhängen, ob ein Unternehmen in den Anwendungsbereich von NIS-2 bzw. des deutschen Umsetzungsgesetzes fällt oder nicht.

- Insoweit ist insbesondere auch für Zulieferer noch folgender Absatz in der NACE Rev. 2 von Bedeutung:[5]

---

[3] Vgl. Anlage 2 des künftigen BSI-Gesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1.

[4] Vgl. S. 170 ff. unter https://ec.europa.eu/eurostat/documents/3859598/5902453/KS-RA-07-015-DE.PDF

[5] Vgl. S. 118 unter https://ec.europa.eu/eurostat/documents/3859598/5902453/KS-RA-07-015-DE.PDF

- *„Die Herstellung von **spezifischen** Teilen, Zubehör und Zusatzvorrichtungen für Maschinen und Geräte wird **generell der gleichen Klasse** zugeordnet wie die Herstellung der entsprechenden Maschinen und Geräte. Die Herstellung von unspezifischen Teilen von Maschinen und Geräten, z. B. Motoren, Kolben, Elektroinstallationsmaterial, Ventile, Getriebe, Kugellager, wird getrennt von den Maschinen und Geräten in den entsprechenden Klassen eingeordnet.“*

- Dies lässt sich nach hiesiger Auffassung so interpretieren, dass ein Zulieferer eines für das Endprodukt (z. B. eine Maschine) maßgeschneiderten Bauteils derselben Klasse zugeordnet wird wie der Hersteller des Endproduktes, während der Zulieferer von eher generischen Bauteilen nicht derselben Klasse zugeordnet werden. Auch dies zeigt, dass die Grenze zwischen einer Betroffenheit von NIS-2 und einer Nicht-Betroffenheit sehr schmal verlaufen kann und im Einzelfall der Interpretation zugänglich sein kann.

- Was die inhaltlichen Anforderungen von NIS-2 bzw. des deutschen Umsetzungsgesetzes angeht, sind betroffene Unternehmen – wie schon unter dem aktuell noch geltenden BSI-Gesetz – verpflichtet, **angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme zu ergreifen,** wobei sie einen umfassenden Anforderungskatalog an sogenannte Cyber-Risikomanagementmaßnahmen zu erfüllen haben (zu diesen später mehr im Kapitel 3).[6]

- Im Falle von „erheblichen Sicherheitsvorfällen“ gelten abgestufte **Meldepflichten** gegenüber dem BSI (vgl. die Tabelle in Kapitel 4).

- Ein „erheblicher Sicherheitsvorfall“ ist ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann (dies wäre wohl in den o. g. fiktiven **Fallbeispielen 1 und 2** der Fall).

Cyber Resilience Act

- Der Cyber Resilience Act ist eine geplante EU-Verordnung, die IT-Sicherheitsanforderungen in Bezug **Produkte und Dienstleistungen mit digitalen Elementen** (z. B. wie im o. g. fiktiven **Fallbeispiel 3,** einem vernetzten Kühlschrank) abzielt.[7] Demnach liegt die Kernverpflichtung für Hersteller solcher Produkte mit digitalen Elementen darin, diese Produkte so zu konzipieren, zu entwickeln und herzustellen, dass sie angesichts der Risiken ein **angemessenes Cybersicherheitsniveau** gewährleisten.

- Die Verordnung soll ab dem Jahr 2027 unmittelbar in allen EU-Mitgliedstaaten gelten.

---

[6] Vgl. § 30 Abs. 2 des künftigen BSI-Gesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

[7] Vgl. den vom Europäischen Parlament am 12.03.2024 angenommenen Vorschlag der Kommission, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.html#title2

- Der Cyber Resilience Act stellt – ähnlich wie NIS-2 in Bezug auf die IT-Sicherheit von Unternehmen – einen Anforderungskatalog an die IT-Sicherheit auf. Allerdings mit dem Unterschied, dass NIS-2 die Cyber-Resilienz der IT-Systeme des Unternehmens insgesamt adressiert, während der Cyber Resilience Act auf eine hinreichende Cyber-Resilienz von **Produkten** mit digitalen Elementen abzielt.

- Im Falle einer „aktiv ausgenutzten Schwachstelle“ und/oder eines „schwerwiegenden Cybersicherheitsvorfalles“ gilt – ähnlich wie bei NIS-2 – ein abgestuftes System mit Meldepflichten.

- Aufgrund der produktspezifischen Zielrichtung des Cyber Resilience Acts und einer Vielzahl an eigenen Besonderheiten muss eine detailliertere Darstellung des Cyber Resilience Acts einem eigenen Papier vorbehalten bleiben. Unternehmen, die in den Anwendungsbereich dieser Verordnung fallen könnten, sollten sich trotz der voraussichtlichen Geltung erst ab 2027 in Anbetracht langer Vorlaufzeiten und Produktzyklen schon bald mit den Anforderungen dieser Verordnung befassen.

2.2 Datenschutzgesetze (DS-GVO, BDSG)

- DS-GVO und BDSG sind von zentraler Bedeutung, wenn es um die Verarbeitung und den Schutz **personenbezogener** Daten geht.

- Art. 32 DS-GVO stellt in Bezug auf die IT-Sicherheit das Herzstück dar. Diese Vorschrift verpflichtet Unternehmen zur Ergreifung **angemessener technischer und organisatorischer Maßnahmen** und stellt damit – flankierend zu den o. g. IT-Sicherheitsgesetzen - Anforderungen an eine hinreichende IT-Sicherheit zum Schutz **personenbezogener** Daten. Verstöße können zu erheblichen Bußgeldern führen.

- Ferner sind Unternehmen verpflichtet, Datenschutzverletzungen innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden (es sei denn, die Verletzung führt „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen“, vgl. Art. 33 DS-GVO, was nach der Systematik des Gesetzes grundsätzlich die Ausnahme darstellen soll).

- Im fiktiven **Fallbeispiel 2** wäre aufgrund der Sensibilität der betroffenen Daten (HR-Daten in erheblichem Umfang) von einer Meldepflicht gegenüber der zuständigen Datenschutz-Aufsichtsbehörde ohne Weiteres auszugehen.

- In diesem fiktiven **Fallbeispiel 2** müssten (vorbehaltlich entgegenstehender Umstände im Einzelfall) wohl auch die betroffenen Personen (also die Mitarbeiter*innen der ElektroInnovate AG) benachrichtigt werden, vgl. Art. 34 DS-GVO. Nach dieser Vorschrift benachrichtigt der Verantwortliche (im **Fallbeispiel 2** also die ElektroInnovate AG) die betroffenen Personen „unverzüglich von der Verletzung, wenn diese voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge hat“. Wann von einem solchen „hohen Risiko“ auszugehen ist, beurteilt sich anhand der konkreten Umstände des Einzelfalles. Eine Orientierung, in welchen Fallgestaltungen Datenschutzbehörden von einem solchen „voraussichtlich hohen Risiko für die betroffenen Personen“ ausgehen, findet sich u. a. unter folgendem Link. Aufgeführt sind eine Vielzahl an Fallgestaltungen im Kontext von Cybervorfällen:

- Leitlinien 01/2021 des EDSA zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf.

- Eine tabellarische Übersicht über die vorgenannten **Melde- und/oder Benachrichtigungspflichten** findet sich in Kapitel 4.

2.3 Vertragliche Verpflichtungen des Unternehmens gegenüber Vertragspartnern

Neben IT-sicherheits- und datenschutzrechtlichen Vorschriften ist an die „allgemeinen Haftungsvorschriften" aus dem Zivilrecht zu denken. Cybervorfälle können vertragliche Haftungsrisiken mit sich bringen, insbesondere, wenn vertragliche Sicherheitsanforderungen nicht eingehalten wurden. Verträge mit Kunden, Lieferanten und Dienstleistern enthalten oft spezifische IT-Sicherheitsanforderungen. Deren Nicht-Einhaltung kann zu Schadensersatzforderungen führen.

2.4 Sorgfaltspflichten und persönliche Haftung der Geschäftsleitung

- Die Unternehmensleitung kann u. U. persönlich haftbar gemacht werden, wenn sie ihre gesellschaftsrechtlich gebotenen Sorgfaltspflichten im Bereich der IT-Sicherheit verletzt. So hat etwa der Geschäftsführer einer GmbH in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden und haftet, soweit er seine Obliegenheiten verletzt, der Gesellschaft im Innenverhältnis für den daraus entstandenen Schaden. Das heißt, dass wenn infolge eines Cybervorfalles ein Schaden eintritt, der hätte verhindert werden können, indem die Gesellschaft die gebotenen IT-sicherheits- und datenschutzrechtlichen Pflichten beachtet hätte, und der Geschäftsführer es schuldhaft vernachlässigt hat, dass seine Gesellschaft diesen Pflichten nachkommen kann, er für den eingetretenen Schaden persönlich in Anspruch genommen werden kann.

- Der im Hinblick auf die konkreten Sorgfaltspflichten der Geschäftsleitung anzulegende Maßstab folgt teils unmittelbar aus den oben genannten Spezialgesetzen. Insbesondere wird im deutschen Umsetzungsgesetz zu NIS-2 die Geschäftsleitung ausdrücklich und wörtlich verpflichtet,

  > *„die nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.*[8]"

- Für den Fall, dass Geschäftsleitungen ihre diesbezüglichen Pflichten verletzen, haften sie ihrem Unternehmen für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts.[9] Dies zieht mittelbar eine **persönliche Haftung** der Geschäftsleitung für eine unzureichende Umsetzung von Cyber-Risikomanagementmaßnahmen aus NIS-2 nach sich.

---

[8] Vgl. § 38 Abs. 1 des künftigen BSI-Gesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

[9] Vgl. § 38 Abs. 2 des künftigen BSI-Gesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

- Übertragen auf das fiktive **Fallbeispiel 1** steht somit eine mögliche persönliche Haftung der Geschäftsführung der StahlTech GmbH für den Schaden im Raum, der aus dem Hacker-Angriff auf das Steuerungssystem resultiert (finanzieller Schaden v. a. aufgrund von Verzögerungen in den Lieferketten).

- Geschäftsleitungen wird daher empfohlen, das Thema IT-Sicherheit sehr ernst zu nehmen und zur Chefsache zu erklären. Ein Delegieren von Verantwortlichkeiten ist möglich, solange dadurch nicht die ureigene Verpflichtung der Geschäftsleitung zur Überwachung der Umsetzung (s. o.) ausgehöhlt wird. Nicht delegierbar ist die Verpflichtung der Geschäftsleitung, selbst regelmäßig an Schulungen teilzunehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von dem Unternehmen erbrachten Dienste beurteilen zu können.[10]

3. Präventiver Schutz – welche präventiven Maßnahmen zum Schutz vor Cybervorfällen müssen Unternehmen ergreifen?

3.1 Cyberrisikomanagementmaßnahmen gemäß den einschlägigen IT-Sicherheitsgesetzen

Die in Kapitel 2 genannten IT-Sicherheitsgesetze verpflichten die jeweils betroffenen Unternehmen zur Ergreifung von präventiven Maßnahmen zum Schutz gegen Cybervorfälle.

Diese Maßnahmen sollen – sowohl gemäß NIS-2 als auch gemäß Cyber Resilience Act – **angemessen** sein und jeweils den **aktuellen Stand der Technik** einhalten. Was im konkreten Einzelfall „angemessen“ ist und dem „Stand der Technik“ entspricht, muss das Unternehmen mit seinen IT-Sachverständigen und/oder seinem IT-Dienstleister bestimmen, begründen und dokumentieren (!).

Mit dem Verweis auf den „aktuellen“ Stand der Technik machen die Gesetze deutlich, dass es sich nicht um eine statische Anforderung handelt, die einmalig und für alle Zukunft erfüllt oder zertifiziert werden kann. Sie verpflichten vielmehr zu einer ständigen Aktualisierungs- und Modernisierungsaufgabe.

Es empfiehlt sich insoweit eine interdisziplinäre Zusammenarbeit zwischen der Rechtsabteilung (oder einem externen Rechtsanwalt) und der IT.

Die konkreten Anforderungen aus NIS-2 bzw. des (insoweit wort- und inhaltsgleichen) deutschen Umsetzungsgesetzes sind in einer **Checkliste in Anlage 1** diesem Leitfaden beigefügt.[11]

---

[10] Vgl. § 38 Abs. 3 des künftigen BSI-Gesetzes, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1

[11] Siehe auch die Hinweise des BSI, wie sich Unternehmen dem Thema NIS-2 annähern können, unter https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html

Die Erfüllung und Einhaltung der geforderten Anforderungen kann unter Berücksichtigung einschlägiger europäischer und internationaler Normen umgesetzt werden. Ein alleiniges Verlassen und ein blanker Verweis auf solche Normen ist allerdings nicht ausreichend. Erforderlich ist, konkret darzulegen und zu dokumentieren, welcher Prüfpunkt einer (z. B. ISO-) Norm die konkrete Anforderung aus dem einschlägigen IT-Sicherheitsgesetz (insbesondere NIS-2) jeweils umsetzt.

In der Praxis empfiehlt sich zur Umsetzung dieser Anforderungen im ersten Schritt die **Durchführung einer Bestandsaufnahme des eigenen IT-Sicherheitsniveaus und einer GAP-Analyse,** z. B. im Rahmen eines **interdisziplinären Workshops zwischen IT, Recht und Geschäftsleitung.** Es bietet sich an, die Bestandsaufnahme und etwaige GAPs in einem Bericht zu dokumentieren und nach einem Maßnahmenkatalog schrittweise abzuarbeiten.

Es ist – wie ausgeführt – zu empfehlen, auf ein interdisziplinäres Team zu setzen, das speziell die Anforderungen des jeweils einschlägigen IT-Sicherheitsgesetzes (insbesondere NIS-2) kennt und insofern die **konkret im Gesetz geforderten Anforderungen mit den Anforderungen an den Stand der Technik „verheiratet".**

3.2 Technische und organisatorische Maßnahmen gemäß den einschlägigen Datenschutzgesetzen

Wie NIS-2 fordert auch die DS-GVO die Ergreifung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik (vgl. Art. 32 DS-GVO). Schutzziel der DS-GVO sind dabei konkret **personenbezogene** Daten. Vieles, was im Rahmen der NIS-2 Compliance umgesetzt wird, lässt sich aber auf die DS-GVO übertragen.

Die konkreten Anforderungen aus der DS-GVO an die technischen und organisatorischen Maßnahmen sind in einer **Checkliste in Anlage 2** diesem Leitfaden beigefügt. Unternehmen sind verpflichtet, die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren (vgl. Art. 5 Abs. 2 DS-GVO). Hierzu dient u. a. die vorgenannte Checkliste, die beliebig erweitert und präzisiert werden kann.

Zu den organisatorischen Maßnahmen gehört es ferner, dass der Datenschutz im Unternehmen so zu organisieren ist, dass in einem möglichen Ernstfall auch die ordnungsgemäße Erfüllung von datenschutzrechtlichen Melde-, Benachrichtigungs- und Dokumentationspflichten sichergestellt ist. Dies ist die Aufgabe der Geschäftsleitung.

Eine ordnungsgemäße Datenschutzorganisation erfordert die klare Benennung interner Zuständigkeiten und konkreter Aufgaben, typischerweise in einer **Leitlinie zum Datenschutz** sowie in internen Richtlinien zur Umsetzung verschiedener datenschutzrechtlicher Anforderungen. Diese schließt auch eine **Richtlinie zum Umgang mit Datenschutzverletzungen** mit ein.
Neben der Abarbeitung der Checkliste in Anlage 2 sind hinsichtlich der präventiven Vorbereitung auf Datenschutzverletzungen folgende Maßnahmen erforderlich:

Maßnahme	Erledigt
Interne Richtlinie zum Umgang mit Datenschutzverletzungen, insbesondere mit Blick auf Melde-, Benachrichtigungs- und Dokumentationspflichten und die damit einhergehenden Risikobeurteilungen.	☐

Checklisten zur systematischen Ermittlung und Dokumentation datenschutzrechtlicher Risiken.	☐
Musterdokument zur ordnungsgemäßen Dokumentation eines Datenschutzvorfalls unter allen datenschutzrechtlich erforderlichen Aspekten.	☐

3.3 Vertragliche Regelungen mit Kunden, Lieferanten, IT-Dienstleistern zur IT-Sicherheit

Als weiterer Baustein für einen präventiven Schutz gegen Cybervorfälle dienen vertragliche Regelungen mit Kunden, Lieferanten, IT-Dienstleistern etc., in denen bestimmte Standards zur IT-Sicherheit konkretisiert werden.

Dies gilt insbesondere für die Bereitstellung von Informationen zur Risikobewertung des Cybersicherheitsniveaus des Vertragspartners, zur Schließung von Sicherheitslücken, zur Erfüllung von Meldepflichten und zur Ermöglichung von Kontrollen und Audits.

Der Inhalt und die erforderlichen Details der Regelungen richten sich nach den für die Vertragsparteien einschlägigen gesetzlichen Regelungen, nach den aus technischer Sicht erforderlichen und im konkreten Vertragsverhältnis angemessenen Maßnahmen zur Cybersicherheit und – wie immer in der Praxis – nach der eigenen Verhandlungsposition, um solche Klauseln in die Verträge aufnehmen zu können.

Vorschläge für mögliche Vertragsklauseln sind der **Checkliste in Anlage 3** diesem Leitfaden beigefügt.

3.4 Abschluss einer Cyberversicherung

Schließlich kann auch eine Cyberversicherung dazu beitragen, Risiken und potenzielle Schäden im Zusammenhang mit Cybervorfällen präventiv zu minimieren, indem sie Unternehmen finanziell absichert und Zugang zu spezialisierten Dienstleistern für Soforthilfe und Schadensbehebung bietet.

Sie unterstützt präventive Maßnahmen, indem sie Unternehmen zu bestimmten Sicherheitsvorkehrungen verpflichtet und Schulungen sowie laufende Phishing-Tests anbietet. Somit dient eine Cyberversicherung nicht nur als finanzielle Absicherung, sondern auch als präventiver Baustein, der Unternehmen hilft, ihre Sicherheitsmaßnahmen zu verbessern und auf Cybervorfälle vorbereitet zu sein.

Bei der Entscheidung, ob und welche Cyberversicherung abgeschlossen werden sollte, müssen Unternehmen mehrere Punkte berücksichtigen. Zunächst sollten sie ihre individuelle Risikosituation und die potenziellen Auswirkungen eines Cybervorfalls auf ihre Geschäftsprozesse analysieren. Es ist wichtig, die bestehenden IT-Sicherheitsmaßnahmen und deren Wirksamkeit zu bewerten. Unternehmen sollten auch die spezifischen Anforderungen und Mindestkriterien der Versicherer prüfen, um sicherzustellen, dass sie diese erfüllen können. Ein Vergleich der verschiedenen Versicherungsangebote, einschließlich der Deckungsumfänge, Prämien und Sublimite, ist unerlässlich.

Wesentliche, dabei zu klärende Fragen sind in einer **Checkliste in Anlage 4** diesem Leitfaden beigefügt.

Zudem sollten Unternehmen die angebotenen Service-Leistungen und Verfügbarkeit von Notfallunterstützung durch spezialisierte Dienstleister berücksichtigen. Letztlich ist es ratsam, sich

ggf. beraten zu lassen um sicherzustellen, dass die gewählte Cyberversicherung den individuellen Bedürfnissen und Risiken des Unternehmens gerecht wird.

4. Repressiver Schutz – Welche repressiven Maßnahmen als Reaktion auf einen Cybervorfall müssen Unternehmen ergreifen?

Während im vorgenannten Kapitel 3 die präventiven Maßnahmen thematisiert wurden, geht es im hiesigen Kapitel 4 um die Ergreifung von repressiven Sofortmaßnahmen im Ernstfall.

Diese wurden in eine **Checkliste** überführt, die als **Anlage 5** diesem Leitfaden beigefügt ist.

Nachfolgend wird auf einige der darin genannten Aspekte eingegangen.

4.1 Beweise sichern

Nach einem Cybervorfall ist es essenziell, alle relevanten Beweise unverzüglich und sorgfältig zu sichern. Dazu gehören Logs, E-Mails, Screenshots und andere digitale Spuren, die den Vorfall dokumentieren. Unternehmen sollten ein forensisches Team beauftragen oder interne IT-Experten einsetzen, um die Integrität der Beweise zu gewährleisten.

Aus rechtlicher Sicht ist die Beweissicherung von entscheidender Bedeutung, weil sie die Grundlage für mögliche rechtliche Schritte und die Erfüllung gesetzlicher Meldepflichten bildet. Ohne ausreichende Beweise können Unternehmen Schwierigkeiten haben, die Ursachen des Vorfalls zu ermitteln, Verantwortlichkeiten zu klären und sich gegen mögliche Schadenersatzansprüche oder Bußgelder zu verteidigen. Zudem sind gesicherte Beweise notwendig, um die Zusammenarbeit mit Strafverfolgungsbehörden zu erleichtern und die Einhaltung gesetzlicher Vorschriften wie der DSGVO und des BSI-Gesetzes nachzuweisen.

4.2 Meldepflichten gegenüber Sicherheits- und Datenschutzbehörden

Unternehmen sind gemäß NIS-2 bzw. dem deutschen Umsetzungsgesetz von NIS-2 (umgesetzt im BSI-Gesetz) sowie der DS-GVO verpflichtet, Cybervorfälle innerhalb bestimmter Fristen den zuständigen Sicherheits- und Datenschutzbehörden zu melden (vgl. hierzu bereits Kapitel 3).

NIS-2/BSI-Gesetz:

Stufe 1: **Frühe Erstmeldung**	Unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, muss eine frühe Erstmeldung abgegeben werden, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte.
Stufe 2: **Bestätigende Erstmeldung**	Unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall,

	muss eine Meldung über den Sicherheitsvorfall abgegeben werden, in der die in Stufe 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie ggf. die Kompromittierungsindikatoren angegeben werden.
Stufe 3: Zwischenmeldung	Auf Ersuchen des BSI muss eine Zwischenmeldung über relevante Statusaktualisierungen getätigt werden.
Stufe 3a: Fortschrittsmeldung	Dauert der Sicherheitsvorfall zum Zeitpunkt der Stufe 4 noch an, legt das betreffende Unternehmen statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vor.
Stufe 4: Abschlussmeldung	Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Stufe 2, vorbehaltlich Stufe 3a, erfolgt eine Abschlussmeldung, die Folgendes enthält: ▪ ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen; ▪ Angaben zur Art der Bedrohung bzw. zu Grunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat; ▪ Angaben zu den getroffenen und laufenden Abhilfemaßnahmen; ▪ die ggf. grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

DS-GVO:[12]

[12] Vorausgesetzt, die materiell-rechtlichen Voraussetzungen der Art. 33 bzw. Art. 34 DS-GVO liegen vor.

Stufe 1: **Meldepflicht gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DS-GVO)**	Unverzüglich und möglichst binnen 72 Stunden nach Kenntniserlangung von der Datenschutzverletzung.
Stufe 2: **Benachrichtigungspflicht gegenüber der betroffenen Person (Art. 34 DS-GVO)**	Unverzüglich. Was heißt das konkret? Die Benachrichtigung sollte „stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der Weisungen“ erfolgen, welche diese oder andere zuständige Behörden, wie bspw. Strafverfolgungsbehörden, geben (ErwGr 86 S. 3 der DS-GVO).
Stufe 3: **Sofern keine Pflicht zur Meldung/Benachrichtigung besteht: Dokumentationspflicht der Datenschutzverletzung (Art. 33 Abs. 5 DS-GVO)**	Diese Dokumentation muss es der Aufsichtsbehörde erlauben zu beurteilen, ob/inwieweit das Unternehmen die Anforderungen der Meldepflicht nach Art. 33 DS-GVO korrekt umgesetzt hat.

4.3 Benachrichtigungspflichten gegenüber Vertragspartnern

Vertragspartner müssen über Cybervorfälle informiert werden, die ihre Daten oder die Erfüllung vertraglicher Verpflichtungen betreffen. Dies kann entweder ausdrücklich vertraglich vorgeschrieben sein (vgl. z. B. die Klauseln in der Checkliste gemäß Anlage 3) oder wegen vertraglicher Schutzpflichten geboten sein. Der Verstoß gegen diese Verpflichtungen kann schadensersatzpflichtig machen. Im Übrigen ist die Benachrichtigung auch deshalb in vielen Fällen geboten, um Transparenz und Vertrauen gegenüber dem Vertragspartner aufrechtzuerhalten.

4.4 Benachrichtigungspflichten gegenüber betroffenen Personen

Insoweit wird verwiesen auf Kapitel 4.2.

4.5 Benachrichtigungspflichten gegenüber Cyberversicherung

Im Falle eines Cybervorfalls muss die Cyberversicherung zeitnah informiert werden, um den Versicherungsschutz nicht zu gefährden. Die spezifischen Anforderungen und Fristen sind in den Versicherungsbedingungen festgelegt.

4.6 Zusammenarbeit mit Polizei/LKA

Es empfiehlt sich zudem die Zusammenarbeit mit Strafverfolgungsbehörden wie der Polizei oder dem Landeskriminalamt (LKA). Eine schnelle und effektive Zusammenarbeit kann dazu beitragen, den Vorfall zu untersuchen, die Täter zu identifizieren und weitere Schäden zu verhindern.

Unter

https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

sind die Kontaktdaten der zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für Wirtschaftsunternehmen genannt. Die einzelnen Länder halten teils eigene hilfreiche Informationen auf ihren Webseiten bereit.

In Hessen kann man sich u. a. unter folgender E-Mail-Adresse an das LKA wenden: zac.hlka@polizei.hessen.de.

Informationen des BKA und Empfehlungen für Wirtschaftsunternehmen zum Umgang mit Cybervorfällen finden Sie hier:

BKA - Cybercrime – Handlungsempfehlungen für Wirtschaftsunternehmen.

4.7 Kommunikation und PR

Eine gut koordinierte Kommunikation ist entscheidend, um die negativen Auswirkungen eines Cybervorfalls auf den Ruf des Unternehmens zu minimieren. Eine durchdachte Kommunikationsstrategie hilft, das Vertrauen von Kunden, Partnern und der Öffentlichkeit zu bewahren. Dabei sollte die Kommunikation schnell, ehrlich und konsistent sein, um Missverständnisse und Spekulationen zu vermeiden.

Die konkrete Strategie hängt aber vom Einzelfall ab und sollte mit einem Kommunikationsprofi **sowie dem Krisenstab** abgestimmt sein.

Denkbar sind folgende Ansätze:

- Eine **proaktive Kommunikation** beinhaltet die aktive und frühzeitige Information der betroffenen Parteien und der Öffentlichkeit über den Vorfall. Dabei werden Fakten offengelegt, ohne Panik zu schüren. Die proaktive Kommunikation signalisiert Transparenz und Verantwortungsbewusstsein, was das Vertrauen in das Unternehmen stärkt. Gegenüber Vertragspartnern kann eine proaktive Kommunikation schon deshalb angezeigt sein, um nicht Gefahr zu laufen, vertragliche Schutzpflichten zu verletzen (s. bereits oben).

- Der proaktive Ansatz birgt aber auch Risiken. Es muss sehr sorgsam abgewogen werden, wie viel „Sachverhalt“ man der Öffentlichkeit und somit auch potenziellen Anspruchstellern (z. B. betroffenen Personen, Vertragspartnern) offenbaren will. In der Praxis ist „weniger manchmal mehr“.

- In keinem Fall sollten ohne Not Dinge kommuniziert werden, aus denen sich Haftungstatbestände ableiten lassen.

- Bei einer **reaktiven Kommunikation** wird zunächst abgewartet und erst auf externe Anfragen oder Berichterstattungen reagiert. Diese Strategie kann sinnvoll sein, wenn noch nicht alle Informationen vorliegen oder das Ausmaß des Vorfalls noch unklar ist. Allerdings birgt sie das Risiko, dass das Unternehmen als intransparent wahrgenommen wird.

- Neben der eigenen Kommunikation sollte ein Unternehmen stets im Blick haben, wie Dritte über den Vorfall berichten und sofern dies die Persönlichkeitsrechte des Unternehmens und/oder von Mitarbeiter*innen oder der Geschäftsleitung verletzen könnte,

erwägen, hiergegen frühzeitig vorzugehen, um die Reputation des Unternehmens und der Betroffenen zu schützen.

5. Lösegeldforderung von Angreifern – zahlen oder nicht?

Zur Frage, ob man auf Lösegeldforderungen von Erpressern eingehen sollte, existiert ein relativ klares, überwiegendes Meinungsbild.

Behörden empfehlen,[13]

- sich im Falle von Erpressungsversuchen grundsätzlich nicht auf Lösegeldzahlungen einzulassen,

- jeden Erpressungsversuch zur Anzeige zu bringen sowie

- das jeweilige Landes-CERT oder das BSI zu informieren.

Insbesondere deshalb, um sich auch für die Zukunft nicht erpressbar zu machen. Im Übrigen kann eine solche Zahlung auch strafrechtliche Relevanz haben (Stichwort: Unterstützung einer kriminellen Vereinigung, §§ 129, 129a StGB).

Der Empfehlung der Behörden schließen sich viele Experten an.

Andererseits wird nicht verkannt, dass es auch Argumente für eine Zahlung geben mag.

Letztlich ist diese Frage in jedem Einzelfall abzuwägen.

6. Fazit

Cybervorfälle stellen eine erhebliche Bedrohung für Unternehmen dar und können weitreichende finanzielle und rechtliche Konsequenzen nach sich ziehen. Der vorliegende Leitfaden hat die verschiedenen Aspekte und notwendigen Maßnahmen zur Prävention und Reaktion auf Cybervorfälle detailliert beleuchtet. Er zeigt auf, dass ein umfassendes Cyberrisikomanagement **nicht nur eine gesetzliche Pflicht, sondern auch eine unternehmerische Notwendigkeit ist.**

Die rechtlichen Anforderungen, die sich aus IT-Sicherheitsgesetzen wie dem BSI-Gesetz und der NIS-2-Richtlinie sowie Datenschutzgesetzen wie der DS-GVO ergeben, verlangen von Unternehmen, präventive Maßnahmen zu ergreifen, um ihre IT-Systeme und personenbezogenen Daten zu schützen. Dazu gehören technische und organisatorische Maßnahmen sowie die Einhaltung von Meldepflichten im Ernstfall. Der Abschluss von Cyberversicherungen kann dabei helfen, finanzielle Risiken zu minimieren und Zugang zu spezialisierten Dienstleistern zu erhalten.

Die präventiven Maßnahmen umfassen unter anderem die Implementierung von Cyberrisikomanagementsystemen, die Durchführung regelmäßiger Schulungen und die Etablierung klarer Richtlinien zur IT-Sicherheit und zum Datenschutz. Durch vertragliche Regelungen mit Geschäftspartnern und die Sicherstellung einer umfassenden Beweissicherung im Ernstfall können Unternehmen ihre rechtliche Position stärken und die Auswirkungen von Cybervorfällen begrenzen.

---

[13] https://polizei.nrw/sites/default/files/2022-05/20220428%20Flyer%20Ransomware%20Internet.pdf

Im repressiven Bereich sind schnelle und koordinierte Reaktionen entscheidend. Dazu gehört die unverzügliche Sicherung von Beweisen, die Meldung an die zuständigen Behörden und die Benachrichtigung betroffener Personen und Vertragspartner. Eine durchdachte Kommunikationsstrategie kann zudem helfen, den Ruf des Unternehmens zu schützen und das Vertrauen der Öffentlichkeit zu bewahren.

Die Investition in präventive Maßnahmen zur Verhinderung von Cybervorfällen zahlt sich aus. Unternehmen, die sich frühzeitig und umfassend der Thematik auseinandersetzen, sind besser gerüstet, um im Ernstfall schnell und effektiv zu reagieren. Dies schützt nicht nur vor finanziellen Verlusten und rechtlichen Konsequenzen, sondern stärkt auch das Vertrauen von Kunden und Geschäftspartnern. **Prävention ist daher nicht nur rechtlich geboten, sondern auch aus unternehmerischer Sicht unverzichtbar.**