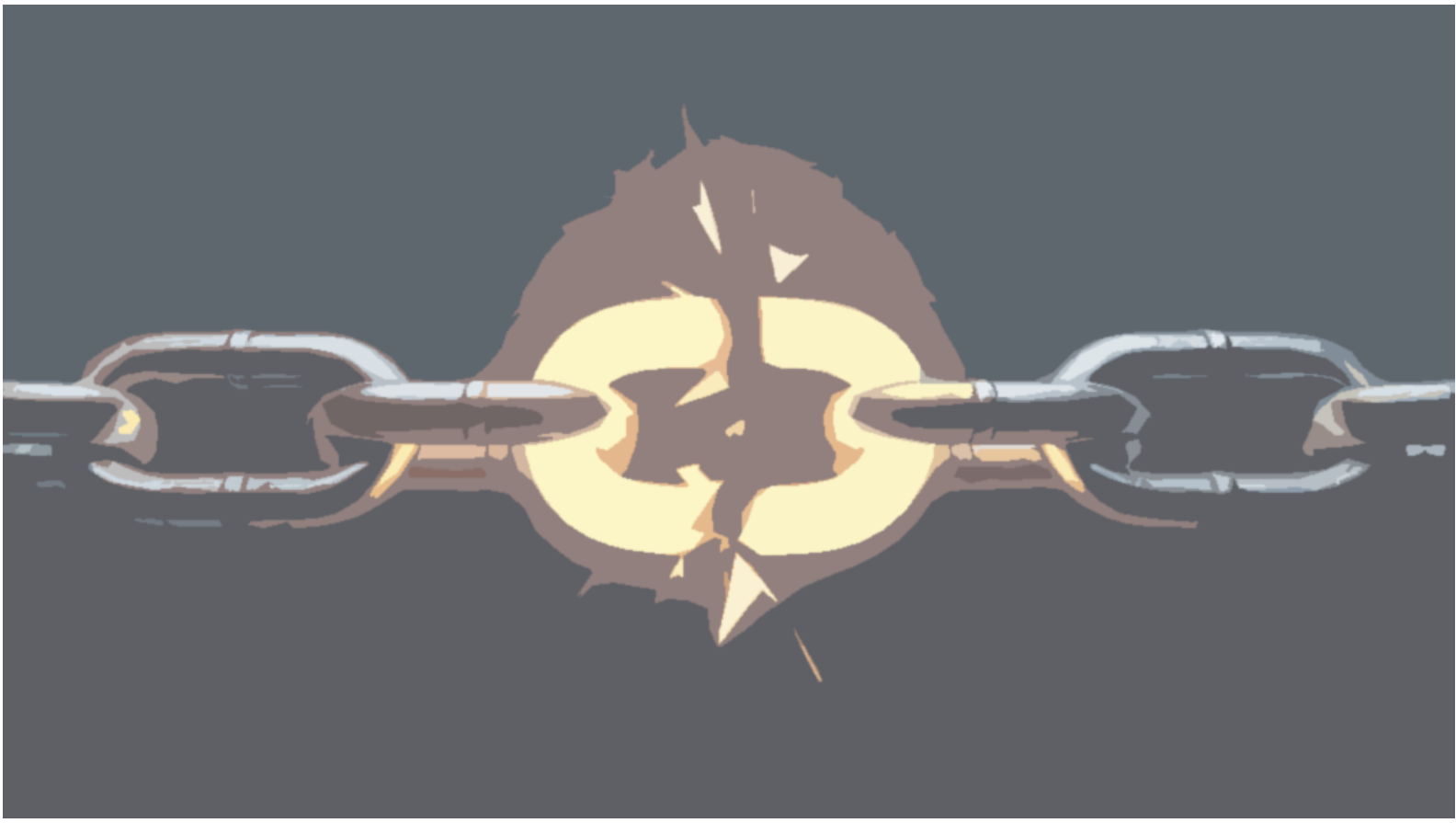
VEREINIGUNG
DER HESSISCHEN
UNTERNEHMERVERBÄNDE

Arbeitsrecht



Die rechtliche Dimension von Cybervorfällen – was Unternehmen präventiv und im Ernstfall 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:

Sabine Prößl
Verband der Metall- und Elektro-Unternehmen Hessen e. V.
Emil-von-Behring-Straße 4, 60439 Frankfurt am Main
T +49 69 95808-183
F +49 69 95808-126
sabine.proessl@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

Hinweise:

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 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 bei Cyberattacken richtig zu handeln. Bestandteil des Leitfadens sind auch mehrere Checklisten, in denen die im Leitfaden angesprochenen Aspekte enthalten sind (z. B. eine Checkliste für rechtliche gebotenen Sofortmaßnahmen im Falle eines Cybervorfalles, Anhang 4).

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

INHALTSVERZEICHNIS

1. Einleitung

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) präventiv 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 haben 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. 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.

Reputation/Kommunikation/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.

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 wird.

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 Steuerungssys-

tem (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.

IT-Sicherheitsgesetze (v. a. BSI-Gesetz, 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/NIS-2 Richtlinie

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

Mittlerweile (Stand Dezember 2025) ist auch das deutsche Umsetzungsgesetz von NIS-2 – ohne Umsetzungsfristen! – in Kraft. Die Vorgaben von NIS-2 werden nunmehr im neuen BSI-Gesetz[2] umgesetzt. Der Anwendungsbereich von NIS-2 wurde gegenüber NIS-1 um einige Wirtschaftssektoren und Bereiche erweitert. Unter anderem wird jetzt auch der Sektor „Verarbeitendes Gewerbe/Herstellung von Waren" von NIS-2 bzw. dem BSI-Gesetz umfasst. Welche Tätigkeiten und Unternehmen konkret hierunter fallen, ist den Anlagen 1 und 2 des BSI-Gesetzes 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 BSI-Gesetzes, wenn sie zusätzlich die vorgesehenen Größen-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. aufweisen.

Es werden nun auch eine Vielzahl an kleinen bis mittelständischen Unternehmen aus der Metall- und Elektroindustrie vom BSI-Gesetz erfasst. Insoweit wird der von NIS-2 erfasste Sektor „Verarbeitendes Gewerbe/Herstellung von Waren" einschlägig sein. Innerhalb dieses Sektors verweist Anlage 2 des BSI-Gesetzes 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 BSI-Gesetz, 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 es 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 BSI-Gesetz 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

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

[2] https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

[3] Vgl. Anlage 2 des BSI-Gesetzes, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html.

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

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 BSI-Gesetzes fällt oder nicht.

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

„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 und im Einzelfall der Interpretation zugänglich sein kann.

Was die inhaltlichen Anforderungen von NIS-2 bzw. des BSI-Gesetzes angeht, sind betroffene Unternehmen 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

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

[6] Vgl. § 30 Abs. 2 des BSI-Gesetzes, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

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 – wie NIS-2 ebenfalls bereits verabschiedete – EU-Gesetzgebung in Form einer EU-Verordnung (nachfolgend CRA), 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 Kernverpflichtungen 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.[8]

Der CRA wird ab dem 11. Dezember 2027 unmittelbar in allen EU-Mitgliedstaaten gelten. Bereits ab dem 11. September 2026 gelten die Pflichten für Hersteller von vernetzten Produkten in Bezug auf sog. aktiv ausgenutzte Schwachstellen gemäß Art. 14 des CRA („Meldepflichten für Hersteller").

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. Die wesentlichen Pflichten für Hersteller von vernetzten Produkten werden in Kapitel 3 dieses Leitfadens dargestellt. 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.

KRITIS-Dachgesetz

Der Bundestag hat mit Beschluss vom 29. Januar 2026 das KRITIS-Dachgesetz verabschiedet.[9] In der regulatorischen Entwicklung dominierte in jüngerer Zeit vor allem die Umsetzung

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402847

[8] Vgl. im Einzelnen die Pflichten für Hersteller von Produkten mit digitalen Elementen: Anlage 1a zu diesem Leitfaden

[9] https://www.recht.bund.de/bgbl/1/2026/66/regelungstext.pdf?__blob=publicationFile&v=1

der NIS-2, die eine große Bandbreite von Unternehmen aus der Metall- und Elektroindustrie betrifft. Vom KRITIS-Dachgesetz betroffen sind hingegen vor allem Betreiber in Sektoren wie Energie, Gesundheit, IT und Telekommunikation, Transport oder Wasser. Ob Unternehmen aus der Metall- und Elektroindustrie hierunter fallen, muss im Einzelfall geprüft werden (im Regelfall eher nein).

Ob eine Anlage als kritisch gilt, bestimmt sich nach sektorspezifischen Schwellenwerten, die an ihre konkrete Versorgungsrelevanz anknüpfen. Maßgeblich ist nicht allein die Größe des Unternehmens, sondern die Bedeutung der jeweiligen Anlage für die Aufrechterhaltung zentraler gesellschaftlicher Funktionen.

Während Ziel von NIS-2 eine belastbare Cyberresilienz der gesamten regulierten Einrichtung ist, zielt das KRITIS-Dachgesetz auf die Aufrechterhaltung des Anlagenbetriebs unter realen Störbedingungen ab (soweit überhaupt eine grundsätzliche Betroffenheit vorliegt). Neben digitalen Angriffen sind insbesondere physische Risiken einzubeziehen, etwa länger andauernde Stromausfälle, der Ausfall externer Versorger, unbefugter Zutritt zu Anlagen oder Naturereignisse. Maßgeblich ist die tatsächliche Betriebsfähigkeit der einzelnen Anlage, nicht allein die IT-Sicherheitslage des Unternehmens. Das KRITIS-Dachgesetz ergänzt die NIS-2 um eine anlagenbezogene Resilienzperspektive. Auch die Aufsichtsstrukturen unterscheiden sich: Während NIS2 primär durch das BSI beaufsichtigt wird, liegt die Zuständigkeit für das KRITIS-Dachgesetz beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
Was ist konkret (für betroffene Unternehmen bzw. Anlagen) zu tun?

- Registrierung beim BBK bis zum 17. Juli 2026
- Benennung einer jederzeit erreichbaren Kontaktstelle
- anlagenspezifische Risikoanalysen
- Erstellung von Resilienzplänen
- Bewertung und Dokumentation von Energieversorgung, baulicher Sicherung, Zugangskontrolle, Redundanzstrukturen und Wiederanlaufprozessen
- Prozesse und Verantwortlichkeiten von Meldeprozessen etablieren.

Datenschutzgesetze (DSGVO, BDSG)

DSGVO und BDSG sind von zentraler Bedeutung, wenn es um die Verarbeitung und den Schutz personenbezogener Daten geht.

Art. 32 DSGVO 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. Eine hilfreiche Checkliste mit möglichen technischen und organisatorischen Maßnahmen zur Verstärkung der IT-Sicherheit gemäß Art. 32 DSGVO hat das Bayerisches Landesamt für Datenschutzaufsicht unter
https://www.lda.bayern.de/media/baylda_checkliste_cyberfestung.pdf

veröffentlicht („Checkliste Cyberfestung“).

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 DSGVO, was nach der Systematik des Gesetzes grundsätzlich die Ausnahme darstellen soll). Die Meldepflichten gemäß DSGVO sind zusätzlich zu denen gemäß dem BSI-Gesetz zu erfüllen.

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 der ElektroInnovate AG) benachrichtigt werden, vgl. Art. 34 DSGVO. 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.

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.

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. Das (neue) BSI-Gesetz schreibt ganz ausdrücklich diese Pflichten für die Geschäftsführung vor und benennt ebenso ganz ausdrücklich eine mögliche persönliche Haftung der Geschäftsführung (vgl. § 38 Abs. 1 und 2 BSI-Gesetz). Demnach wird die Geschäftsleitung ausdrücklich und wörtlich verpflichtet, *„die nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.*[10]*“*

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.[11] Dies zieht mittelbar eine persönliche Haftung der Geschäftsleitung für eine unzureichende Umsetzung von Cyber-Risikomanagementmaßnahmen aus NIS-2 nach sich.

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

[10] Vgl. § 38 Abs. 1 des BSI-Gesetzes, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

[11] Vgl. § 38 Abs. 2 des BSI-Gesetzes, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

regelmäßig an Schulungen teilzunehmen (vgl. § 38 Abs. 3 BSI-Gesetz), 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.[12]

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

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. Sie richten sich im Übrigen nach den Umständen und dem Schutz. Bedarf der Infrastruktur und/oder des Produktes im konkreten Einzelfall.

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) BSI-Gesetzes sind in einer Checkliste in Anlage 1 zu diesem Leitfaden beigefügt.[13] Es handelt sich dabei aber nur um eine grobe Checkliste und erste Basisfragen. Die konkreten Anforderungen aus dem CRA für Hersteller von Produkten mit digitalen Elementen sind in einer Auflistung in Anlage 1a zu diesem Leitfaden beigefügt.

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

[12] Vgl. § 38 Abs. 3 des BSI-Gesetzes, https://www.gesetze-im-internet.de/bsig_2025/BJNR12D0B0025.html

[13] 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

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".

Technische und organisatorische Maßnahmen gem. den einschlägigen Datenschutzgesetzen

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

Die konkreten Anforderungen aus der DSGVO an die technischen und organisatorischen Maßnahmen sind in einer Checkliste in Anlage 2 zu diesem Leitfaden beigefügt. Diese Checkliste kann mit der „Checkliste Cyberfestung" des Bayerisches Landesamtes für Datenschutzaufsicht verknüpft oder ergänzt werden.[14] Unternehmen sind zudem verpflichtet, die ergriffenen technischen und organisatorischen Maßnahmen zu dokumentieren (vgl. Art. 5 Abs. 2 DSGVO). Hierzu dienen u. a. die vorgenannten Checklisten, die unternehmens- und kontextspezifisch erweitert und präzisiert werden können.

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.

---

[14] https://www.lda.bayern.de/media/baylda_checkliste_cyberfestung.pdf

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.	☐

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 zu diesem Leitfaden beigefügt.

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 zu 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 zu diesem Leitfaden beigefügt ist. Darüber hinaus enthält dieser Leitfaden den Vordruck einer Organisationsanweisung und Checkliste zur Erfüllung von Melde- und Benachrichtigungspflichten sowohl nach BSI-Gesetz als auch nach DSGVO. Dieses Dokument ist dem Leitfaden als Anlage 6 beigefügt.

Nachfolgend wird auf einige der darin genannten Aspekte eingegangen.

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.

Meldepflichten gegenüber Sicherheits- und Datenschutzbehörden

Unternehmen sind gemäß NIS-2 bzw. dem deutschen Umsetzungsgesetz von NIS-2 (umgesetzt im BSI-Gesetz) sowie der DSGVO 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.

DSGVO:[15]

Stufe 1 - Meldepflicht gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DSGVO)	Unverzüglich und möglichst binnen 72 Stunden nach Kenntniserlangung von der Datenschutzverletzung.
Stufe 2 – Benachrichtigungspflicht gegenüber der betroffenen Person (Art. 34 DSGVO)	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 DSGVO).
Stufe 3 – Sofern keine Pflicht zur Meldung/Benachrichtigung besteht: Dokumentationspflicht der Datenschutzverletzung (Art. 33 Abs. 5 DSGVO)	Diese Dokumentation muss es der Aufsichtsbehörde erlauben, zu beurteilen, ob/inwieweit das Unternehmen die Anforderungen der Meldepflicht nach Art. 33 DSGVO korrekt umgesetzt hat.

[15] Vorausgesetzt, die materiell-rechtlichen Voraussetzungen der Art. 33 bzw. Art. 34 DSGVO liegen vor.

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.

Benachrichtigungspflichten gegenüber betroffenen Personen

Insoweit wird verwiesen auf Kapitel 4.2.

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.

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.

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 Mitarbeitern 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,[16]

- 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.

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 DSGVO 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 Ge-

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

schäftspartnern und die Sicherstellung einer umfassenden Beweissicherung im Ernstfall können Unternehmen ihre rechtliche Position stärken und die Auswirkungen von Cybervorfällen begrenzen.

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.

Anhang

Anlage 1: Checkliste bzgl. Anforderungen der NIS-2/des BSI-Gesetzes
Anlage 1a: Checkliste bzgl. Anforderungen des CRA
Anlage 2: Checkliste bzgl. TOMs gemäß DSGVO
Anlage 3: Mögliche Vertragsklauseln in der Lieferkette
Anlage 4: Checkliste bzgl. Abschluss einer Cyberversicherung
Anlage 5: Checkliste bzgl. Sofortmaßnahmen im Falle eines Cybervorfalles
Anlage 6: Organisationsanweisung und Checkliste zur Erfüllung der Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen (Art. 33, 34 DSGVO) und bei erheblichen Sicherheitsvorfällen (§ 32 BSI-Gesetz)

Anlage 1 - Checkliste NIS-2

Anforderungen aus NIS-2	Beschreibung	Erledigt
Konzept in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	Dies umfasst, dass Sie eine Risikoanalyse und Bestandsaufnahme in Bezug auf Ihre IT-Sicherheit vornehmen, u. a. - Was sind die Risiken? Wie wahrscheinlich sind die Risiken? Sind diese Risiken dokumentiert? - Welche Planungen hat Ihr Unternehmen getroffen, um die Informationssicherheit während einer Störung auf einem angemessenen Niveau aufrechtzuerhalten? - Welche Strategien und Verfahren sind implementiert, um kritische Funktionen und Daten während solcher Ereignisse zu schützen, und wie werden diese Pläne regelmäßig getestet und aktualisiert?	☐
Bewältigung von Sicherheitsvorfällen	Dies umfasst das Aufstellen und Erproben eines Notfallplanes für Cybervorfälle und Datenpannen. - Welche Verfahren wurden implementiert, um Informationssicherheitsvorfälle zu erfassen, zu quantifizieren und zu überwachen?	☐
Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	Dies umfasst die Klärung u. a. folgender Fragen: - Wo befinden sich die Back-ups? Wie weit reichen sie zurück? Wer kann sie anfordern und wie schnell können sie wiederhergestellt werden? - Wie hat Ihr Unternehmen die Handhabung von Informationssicherheitsvorfällen geplant und vorbereitet? Welche Prozesse, Rollen und Verantwortlichkeiten wurden definiert und wie werden diese innerhalb der Organisation kommuniziert? Gibt es regelmäßige Schulungen oder Übungen, um sicherzustellen, dass alle Mitarbeiter mit diesen Prozessen vertraut sind?	☐

Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen Unternehmen und ihren unmittelbaren Anbietern oder Diensteanbietern	Dies umfasst die Überprüfung der Sicherheit der Lieferketten, u. a. - Sind alle Ihre Hauptlieferanten so gut aufgestellt wie Ihr Unternehmen? Oder weiß Ihr Lieferant überhaupt, was Sie von ihm erwarten, und verlassen Sie sich ausschließlich auf die Selbsterklärung des Lieferanten?). Ferner umfasst dies ggf. die vertragliche Verpflichtung Ihrer Vertragspartner zur Erfüllung umfangreicherer IT-sicherheitsrechtlicher Pflichten. - Welche Prozesse und Verfahren hat Ihre Organisation implementiert, um die Informationssicherheitsrisiken zu identifizieren und zu steuern, die mit der Nutzung der Produkte oder Dienstleistungen von Lieferanten verbunden sind? Wie wird sichergestellt, dass diese Verfahren regelmäßig überprüft und an veränderte Risikolagen angepasst werden?	☐
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen	Die hängt mit dem obersten Punkt (Risikoanalyse) zusammen. Schwachstellen sind zu beheben. - Wie überwacht Ihr Unternehmen Netzwerke, Systeme und Anwendungen auf anormales Verhalten, um potenzielle Informationssicherheitsvorfälle frühzeitig zu erkennen? Welche Prozesse sind implementiert, um diese Vorfälle zu bewerten und entsprechende Maßnahmen zur Eindämmung und Behebung zu ergreifen?	☐
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	Dies erfordert regelmäßige Bestandsaufnahmen.	☐
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	Dies erfordert regelmäßige Mitarbeiterschulung im Bereich der Cybersicherheit (U. a. Wie oft und wie intensiv schulen Sie oder sind Ihre Mitarbeiter bereits schulungsmüde? Wann ist eine Online-Schulung ausreichend?	☐

	Nutzen Sie die Möglichkeit, Mitarbeiter durch Schulungen zu Ihrer wichtigsten Verteidigungslinie zu entwickeln?)	
Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung	Entsprechen die Schlüssellängen und Technologien noch dem aktuellen Stand der Technik?	☐
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	Haben Sie ein aktuelles Berechtigungs- und Rollenkonzept? Wie oft überprüfen Sie, ob es aktuell ist?	☐
Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung		☐

Anlage 1a - Anforderungen CRA für Hersteller

Zu den umfassenden Anforderungen des Cyber Resilience Acts an die Cybersicherheit von Softwareprodukten und vernetzten Hardwareprodukten für den Hersteller gehören beispielsweise Risikoanalysen, Cybersicherheitskonfigurationen des Produkts und Meldepflichten gegenüber Behörden und Nutzern. Produkte müssen für einen Zeitraum von mindestens 5 Jahren, teilweise auch länger, mit Sicherheitsupdates versorgt werden. Der Hersteller muss vor dem Inverkehrbringen eines Produkts ein internes (teilweise auch externes) Kontrollverfahren durchlaufen. Er muss eine EU-Konformitätserklärung ausstellen und die Produkte mit der sogenannten „CE“-Kennzeichnung versehen.

Die Folgende Aufzählung beinhaltet die wesentlichen Pflichten für den Hersteller (ohne Anspruch auf abschließende Vollständigkeit):

- Festlegung eines **Unterstützungszeitraums** für das Produkt, regelmäßig mind. 5 Jahre (Art. 13 Absätze 8 und 19 CRA)
- Aufstellung, Dokumentation und Aktualisierung einer Bewertung der Cybersicherheitsrisiken („**Risk Assessment**“) (Art. 13 Absätze 2 und 3 CRA)
- Konzeption, Entwicklung und Herstellung des Produkts gemäß den „**grundlegenden Cybersicherheitsanforderungen**“ in Anhang I Teil I des CRA:
    - Gewährleistung eines risikoangemessenen Cybersicherheitsniveaus im Allgemeinen,
    - Bereitstellung des Produkts ohne bekannte Schwachstellen,
    - Secure-by-Default-Konfiguration des Produkts,
    - Möglichkeit von (automatischen) Sicherheitsupdates,
    - Schutz vor unbefugtem Zugriff, darunter zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und Meldung von unbefugten Zugriffen,
    - Gewährleistung der Vertraulichkeit von Daten, z. B. durch Verschlüsselung,
    - Gewährleistung der Integrität von Daten, Befehlen, Programmen und Konfigurationen und Meldung von Manipulationen,
    - Konzeption, Entwicklung und Herstellung des Produkts nach dem Grundsatz der Datenminimierung,
    - Gewährleistung der Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall,
    - Minimierung der negativen Auswirkungen auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste,
    - Konzeption, Entwicklung und Herstellung des Produkts mit möglichst geringer Angriffsfläche,
    - Konzeption, Entwicklung und Herstellung des Produkts, so dass die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,

  - Bereitstellung sicherheitsbezogener Informationen durch Aufzeichnung und/oder Überwachung interner Vorgänge wie Zugriffe auf Daten oder Funktionen, inkl. Opt-out-Mechanismus für Nutzer,
  - Möglichkeit für den Nutzer, alle Daten und Einstellungen dauerhaft sicher und einfach zu löschen, und, wenn diese Daten auf andere Produkte oder Systeme übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht.

- **„Due Dilligence", wenn Hersteller Drittanbieter-Komponenten** in ihre Produkte integrieren, sodass solche Komponenten die Cybersicherheit des Produkts nicht beeinträchtigen;
- **Schwachstellenbehandlung im Einklang mit den grundlegenden Cybersicherheitsanforderungen** in Anhang I Teil II:
  - Ermittlung und Dokumentation der Schwachstellen und Komponenten der Produkte, u. a. durch Erstellung einer Software-Stückliste („SBOM") in einem gängigen maschinenlesbaren Format, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;
  - Unverzügliche Behandlung von Schwachstellen, unter anderem durch Bereitstellung von Sicherheitsaktualisierungen,
  - Regelmäßige Überprüfung und Test der Sicherheit des Produkts,
  - Bereitstellung von Nutzerinformationen über Sicherheitsaktualisierungen und Schwachstellen,
  - Aufstellen und Umsetzung einer Strategie für die koordinierte Offenlegung von Schwachstellen,
  - Maßnahmen für den Austausch von Informationen über mögliche Schwachstellen, u. a. eine Kontaktadresse für die Meldung der entdeckten Schwachstellen;
  - Mechanismen für die sichere Verbreitung von Aktualisierungen, damit Schwachstellen rechtzeitig und im Falle von Sicherheitsaktualisierungen gegebenenfalls automatisch behoben oder eingedämmt werden;
  - Bereitstellung von in der Regel kostenlosen Sicherheitsaktualisierungen zusammen mit Hinweisen und einschlägigen Informationen an den Nutzer.
- **Bereithalten von früheren Sicherheitsupdates** für mind. 10 Jahre (Art. 13 Abs. 8 CRA);
- **Meldung von Schwachstellen an Drittkomponentenhersteller** (Art. 13 Abs. 6 CRA);
- Aufstellen und Bereithalten einer **technischen Dokumentation** zu dem Produkt (Art. 13 Absätze 12, 13 und Art. 31 und Annex VII CRA);
- Durchlaufen des einschlägigen **Konformitätsbewertungsverfahrens** und Erstellung der **EU-Konformitätserklärung** sowie Anbringen des **CE-Kennzeichens;**
- Bereitstellung von **Nutzerinformationen und -Anleitungen** (Art. 13 Absätze 15 bis 18 CRA);
- **Meldung** von aktiv ausgenutzten Schwachstellen und erheblichen Sicherheitsvorfällen **gegenüber der ENISA und dem nationalen CSIRT** (Art. 14 CRA);
- **Meldung** von aktiv ausgenutzten Schwachstellen und erheblichen Sicherheitsvorfällen **gegenüber betroffenen oder allen Nutzern** (Art. 14 Abs. 8 CRA);

Anlage 2 - Checkliste technische und organisatorische Maßnahmen nach Art. 32 DSGVO[17]

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Schlüsselregelung/Liste
☐ Biometrische Zugangssperren	☐ Empfang/Rezeption
☐ Chipkarte/Transpondersysteme	☐ Besucherkontrolle/Protokollierung
☐ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
	☐ Sorgfalt bei Auswahl Reinigungsdienste

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Login mit Benutzername & Passwort	☐ Verwalten von Benutzerberechtigungen
☐ Firewall	☐ Erstellen von Benutzerprofilen
☐ Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
☐ Anti-Viren-Software Clients	☐ Richtlinie „Sicheres Passwort“
☐ Intrusion Detection Systems	☐ Allgemeine Richtline Datenschutz und/oder Sicherheit
☐ Mobile Device Management	
☐ Einsatz von VPN bei Remote-Zugriffen	
☐ BIOS Schutz (separates Passwort)	
☐ Automatische Desktopsperre	
☐ Verschlüsselung von Notebooks/Tablets	

1.3. Zugriffskontrolle

[17] Kann durch die „Checkliste Cyberfestung“, abrufbar unter https://www.lda.bayern.de/media/baylda_checkliste_cyberfestung.pdf, ergänzt werden.

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Aktenshredder (mind. Stufe 3, cross cut)	☐ Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (insb. DIN 66399)	☐ Minimale Anzahl an Administratoren
☐ Physische Löschung von Datenträgern	☐ Datenschutztresor

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung von Produktiv- und Testumgebung	☐ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme/Datenbanken/Datenträger	☐ Festlegung von Datenbankrechten

2. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann an, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von VPN	
☐ Protokollierung der Zugriffe und Abrufe	

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Feuer- und Rauchmeldeanlagen	☐ Backup & Recovery-Konzept
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherheitsmedien an einem sicheren Ort außerhalb des Serverraums
☐ Serverraum Löschanlage	☐ Kontrolle des Sicherheitsvorgangs
☐ USV	
☐ Schutzsteckdosenleisten Serverraum	
☐ RAID System/Festplattenspiegelung	

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	
	☐ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	☐ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich

4.2. Vorfall- und Reaktions-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	
☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	
☐ Einsatz von Virenscanner und regelmäßige Aktualisierung	
☐ Intrusion Detection System (IDS)	
☐ Intrusion Prevention System (IPS)	

4.3. Datenschutzfreundliche Voreinstellung (Art. 25 Abs. 2 DSGVO)

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☐ Einfache Ausübung der Betroffenenrechte durch technische Maßnahmen	

4.4. Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
	☐ Regelung zum Einsatz weiterer Subunternehmer

Anlage 3 - Mögliche Vertragsklauseln im Bereich Cyber- und Informationssicherheit[18]

(1) Der Auftragnehmer ergreift geeignete und verhältnismäßige technische und organisatorische Maßnahmen, um die im Zusammenhang mit den bereitgestellten Produkten und/oder Dienstleistungen gespeicherten Daten des Auftraggebers und dessen Netz- und Informationssysteme gegen unbefugten Zugriff zu schützen und die Auswirkungen von Sicherheitsvorfällen auf den Auftraggeber zu verhindern oder möglichst gering zu halten. Der Auftragnehmer setzt hierbei den neuesten Stand der Technik ein. Ein Sicherheitsvorfall ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt.

(2) Der Auftragnehmer stellt dem Auftraggeber auf dessen Anforderung sämtliche Informationen zur Verfügung, die dieser zur Durchführung und Dokumentation einer Bewertung der Risiken für die Cyber- und Informationssicherheit benötigt. Der Auftraggeber kann die Einhaltung der im vorgenannten Absatz niedergelegten Pflicht des Auftragnehmers durch die Einholung von Auskünften und Abfrage von Nachweisen beim Auftragnehmer in Form von marktüblichen Zertifizierungen und/oder Eigenerklärungen des Auftragnehmers kontrollieren.

(3) Der Auftragnehmer informiert den Auftraggeber im Falle eines Sicherheitsvorfalls unverzüglich auf elektronischem Wege und unterrichtet ihn unaufgefordert und fortlaufend über die zur Aufklärung und Behebung des Vorfalls getroffenen Maßnahmen.

(4) Der Auftragnehmer stellt im Falle von ihm mitgeteilten oder öffentlich bekannt gewordenen Sicherheitslücken unverzüglich und unentgeltlich ein Sicherheits-Update zur Verfügung oder ergreift sämtliche sonstigen Maßnahmen, die die Sicherheitslücke beseitigen.

(5) Der Auftragnehmer erstellt [Häufigkeit der Back-ups, z. B. „stündlich“ oder „täglich um 0:00 Uhr“] mindestens [Anzahl, z. B. „zwei“] Back-ups der Daten des Auftraggebers und speichert die Daten georedundant. Es müssen jederzeit mindestens [Anzahl, z. B. „fünf“] Back-ups der letzten [Anzahl, z. B. „zwei Monate“] bereitgehalten werden. Das Back-up ist im Einzelnen wie folgt ausgestaltet [technische Beschreibung des Back-ups sowie der technischen Voraussetzungen, z. B. differenzielle oder inkrementelle Back-ups].

(6) Der Auftragnehmer arbeitet auf erstes Anfordern mit den für den Auftraggeber zuständigen Aufsichtsbehörden zusammen, ermöglicht Kontrollen der Behörden vor Ort und unterstützt den Auftraggeber angemessen bei behördlichen Kontrollmaßnahmen.

(7) Der Auftragnehmer wird den Auftraggeber auf erstes Anfordern von allen Forderungen und Ansprüchen freistellen und gegen alle Ansprüche verteidigen, die wegen der Verletzung seiner in den vorgenannten Absätzen niedergelegten Pflichten durch Dritte geltend gemacht werden. Der Auftragnehmer erstattet dem Auftraggeber alle entstehenden Verteidigungskosten und sonstigen Schäden.

[18] Diese Klauseln bieten bloß Anregungen und sind unbedingt auf den jeweiligen Einzelfall anzupassen.

Anlage 4

Maßnahme	Erledigt
Sind Schäden wegen Betriebsunterbrechung mitversichert und bis zu welchem Limit?	☐
Sind Fremdschäden bzw. Ansprüche von Dritten, gerichtet auf u. a. Erfüllung des Vertrages oder auf Zahlung von Schadensersatz wegen Nichterfüllung des Vertrages, mitversichert und bis zu welchem Limit? (gerade Ansprüche, die Vertragspartner wegen der Nicht-/Schlecht-erfüllung eines Vertrages geltend machen, sind eines der Hauptrisiken eines Cyberangriffes und werden häufig auch nicht vom Betriebsun-terbrechungsschaden vollständig aufgefangen, der häufig lediglich den entgehenden Betriebsgewinn und den Aufwand an fortlaufenden Kosten adressiert)	☐
Sind Schäden für Datenschutzverletzungen mitversichert und bis zu welchem Limit?	☐
Ist die dienstliche Nutzung privater Geräte mitversichert?	☐
Sind Erpressungsgelder mitversichert?	☐
Sind Kosten für den Wiederaufbau/Wiederherstellung von IT-Infrastruktur mitversichert und bis zu welchem Limit?	☐
Sind Kosten für (eigens beauftragte) IT-Forensiker mitversichert und bis zu welchem Limit?	☐
Sind Kosten für (eigens beauftragte) Rechtsanwälte mitversichert und bis zu welchem Limit?	☐
Sind Tochtergesellschaften mitversichert?	☐
Welche Anforderungen stellt die Versicherung an die vorvertraglichen Anzeigenpflichten/Obliegenheiten sowie den vorvertraglich zu erfüllen-den IT-Sicherheitsstandard und kann mein Unternehmen diese Vorga-ben realistisch erfüllen?	☐

Anlage 5 - (Auch rechtlich gebotene) Sofortmaßnahmen bei einem Cybervorfall

Die folgende Checkliste gibt einen Überblick über die typischen, rechtlich gebotenen und sinnvollen Maßnahmen im Fall eines Cybervorfalles. Sie ersetzt allerdings keinen individuellen Notfallplan, der stets anhand der spezifischen Besonderheiten des einzelnen Unternehmens zu erstellen ist. Die Checkliste dient aber auch als Basis, um einen individuellen Notfallplan aufzusetzen. Jedes Mitglied des Krisenstabs sollte diese Checkliste/den (zu erstellenden) Notfallplan in physischer Form aufbewahren.

PRIO 1 – Maßnahmen

Maßnahme	Beschreibung	Erledigt
Krisenstab informieren	Informieren Sie Ihren Krisenstab, üblicherweise bestehend aus ▪ Leiter IT ▪ Rechtsabteilung ▪ Compliance ▪ Datenschutz. Beauftragter ▪ Kommunikation/PR-Abteilung ▪ _____ Kontaktadressen: _____	☐
Sachverhalt sammeln	Tragen Sie Sachverhaltsinformationen und Fakten zum Cybervorfall zusammen Was ist passiert? ▪ Phishing ▪ Malware ▪ Ransomware ▪ DDoS-Angriffe ▪ SQL-Injection ▪ Cross-Site Scripting (XSS) ▪ Credential Stuffing ▪ Social Engineering ▪ Spyware ▪ Eavesdropping ▪ Unbekannt ▪ _____	☐

Maßnahme	Beschreibung	Erledigt
	Klären Sie, ob der Cybervorfall andauert.	☐
	Klären Sie, ob es sich vermutlich um einen vorsätzlichen Angriff handelt oder um einen (zufälligen) Netzwerk-, Hardware- oder Softwarefehler.	☐
	Klären Sie, wie sich der Vorfall ereignet hat. Stellen Sie sicher, dass Sie hierzu Fakten sammeln und verhindern Sie das Kursieren von Vermutungen und Gerüchten. Tätigen Sie in diesem Stadium keine externe Kommunikation, die nicht im Krisenstab abgestimmt ist.	☐
	Klären Sie insbesondere folgende Punkte ▪ Welche Systeme sind betroffen? ▪ Welche Datenkategorien sind betroffen (z. B. Daten von Kunden oder Geschäftspartnern, personenbezogene Daten, Geschäftsgeheimnisse, etc.)?	☐
	Welche negativen Auswirkungen auf den Geschäftsbetrieb sind zu erwarten?	☐
	Informieren Sie alle Mitglieder des Krisenstabs über die Erkenntnisse.	☐
Weitere Personen informieren	Informieren Sie Ihren technischen Berater/IT-Dienstleister/IT-Forensiker Kontaktadressen: _____	☐
	Informieren Sie Ihre Rechtsabteilung und/oder Ihre Anwaltskanzlei Kontaktadressen: _____	☐
	Informieren Sie Ihre Cyberversicherung und sonstige in Betracht kommenden Versicherungen	☐
	Informieren Sie betroffene Mitarbeiter Achtung: Wegen Art. 34 DSGVO unbedingt nur in Abstimmung mit Krisenstab und insbesondere Legal!	☐

	Benachrichtigen Sie ggf. andere relevante Dritte z. B. den Hersteller oder Entwickler der betroffenen Systeme; diese können Ihnen unter Umständen auch bei technischen Notfallmaßnahmen helfen. Achtung: Wegen Art. 34 DSGVO unbedingt nur in Abstimmung mit Krisenstab und insbesondere Legal!	☐
Was ist noch zu tun?	Leiten Sie Notfallmaßnahmen unter Berücksichtigung interner Notfallrichtlinien und -pläne ein, insbesondere zur schnellstmöglichen Beendigung des Angriffs, zur Beweissicherung sowie zur Wiederherstellung von IT-Systemen/Daten (hierzu gehört als erster Schritt, die entsprechenden Ansprechpartner zu informieren, s.o.).	☐

PRIO 2 – Maßnahmen[19]

Meldepflichten nach NIS-2/BSIG gegenüber BSI

Meldestufen	Beschreibung	Erledigt
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.	☐

[19] Siehe hierzu die eigene Organisationsanweisung und Checkliste in Anlage 6 zu diesem Leitfaden

Stufe 4 – Abschluss-meldung	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.	☐

Meldepflichten nach DSGVO gegenüber Aufsichtsbehörden und betroffenen Personen

Meldestufen	**Beschreibung**	**Erledigt**
Stufe 1 - Meldepflicht gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DSGVO)	Unverzüglich und möglichst binnen 72 Stunden nach Kenntniserlangung von der Datenschutzverletzung.	☐
Stufe 2 – Benachrichtigungspflicht gegenüber der betroffenen Person (Art. 34 DSGVO)	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 DSGVO).	☐
Stufe 3 – Sofern keine Pflicht zur Meldung/Benachrichtigung besteht: Dokumentationspflicht der Datenschutzverletzung (Art. 33 Abs. 5 DSGVO)	Diese Dokumentation muss es der Aufsichtsbehörde erlauben, zu beurteilen, ob/inwieweit das Unternehmen die Anforderungen der Meldepflicht nach Art. 33 DSGVO korrekt umgesetzt hat.	☐

PRIO 3 – Maßnahmen

Maßnahme	Erledigt
Prüfen Sie, ob/inwieweit der Cyber-Angriff öffentlich bekannt wurde. Wenn ja, oder die Möglichkeit eines Bekanntwerdens besteht, erarbeiten Sie ein Kommunikationskonzept. Erwägen Sie presse-/äußerungsrechtliche Maßnahmen zum Schutz des Unternehmens und in den Fokus geratener Mitarbeiter/Geschäftsleitung	☐
Prüfen Sie gemeinsam mit der Rechtsabteilung und/oder externen Anwälten die Möglichkeiten einer Anspruchsverfolgung und Anspruchsverteidigung	☐
Maßnahmen zur sofortigen Verbesserung der IT-Sicherheit umsetzen	☐

Anlage 6

Organisationsanweisung und Checkliste zur Erfüllung der Melde- und Benachrichtigungspflichten

- bei Datenschutzverletzungen nach Art. 33, 34 DSGVO und
- bei erheblichen Sicherheitsvorfällen nach § 32 BSI-Gesetz

DATUM

Impressum

Dokumenten Nr.: **[…]**
Datum: **[…]**

Geltungsbereich:

[Name Unternehmen]

Ansprechpartner:

[…]

Datenschutzbeauftragter:

[...]

A. Organisationsanweisung für das Vorgehen bei Datenschutzverletzungen und/oder IT-Sicherheitsvorfällen[20]

I. An wen richtet sich diese Organisationsanweisung?

Diese Organisationsanweisung richtet sich an alle Mitarbeiter von UNTERNEHMEN (nachfolgend „UNTERNEHMEN“).

II. Welchen Zweck hat diese Organisationsanweisung?

Diese Organisationsanweisung hat den Zweck, dass UNTERNEHMEN seinen gesetzlichen Meldepflichten im Falle von Datenschutzverletzungen und/oder IT-Sicherheitsvorfällen gemäß DSGVO und BSI-Gesetz (nachfolgend gemeinsam „Vorfall“ genannt) nachkommen kann.

III. Was sind mögliche Vorfälle?

= Jedes (potenzielle) Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten (einschließlich personenbezogener Daten) oder der Dienste, die über IT-Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt.

Beispiele:

- (Potenzieller) Hackerangriff auf die IT-Systeme und Abzug von Daten
- Phishing-Versuche
- Ransomware
- jeder unvorhergesehene (potenzielle) Verlust von Daten
- fehlerhafte Verteilung von Zugriffsberechtigungen auf Laufwerke
- versehentlicher elektronischer Versand einer unverschlüsselten Liste mit Daten an einen unrechtmäßigen Empfänger
- versehentlicher postalischer Versand von Dokumenten an den falschen Adressaten
- Verwendung von geschäftlichen Daten für private Zwecke
- Verlust oder Diebstahl des Laptops oder eines anderen Datenträgers, wenn die Daten darauf nicht oder nicht ausreichend verschlüsselt sind
- Verlust oder Diebstahl einer Videokamera und des Aufzeichnungsmaterials
- Veröffentlichungen von Daten im Internet aufgrund eines technischen Fehlers
- etc.

[20] Dieser Teil A. richtet sich an alle Mitarbeiter des Unternehmens; Auch wenn männliche Ausdrucksformen verwendet werden, so richtet sich dieses Dokument in gleichem Maße an alle Geschlechter.

IV. Was ist im Falle eines (möglichen) Vorfalles zu tun?

Zunächst – als Erstes! – sind die internen Kontaktpersonen auf schnellstem Wege (Telefonisch; zusätzlich per E-Mail) zu kontaktieren und über den Vorfall zu informieren. Die Kontaktperson gibt dann vor, wie weiter zu verfahren ist.

Dies gilt auch im Falle eines bloßen Verdachts.

Sodann soll der interne Meldebogen (siehe Ziffer VI.) ausgefüllt werden. Dieser ist von demjenigen Mitarbeiter, dem der Vorfall als erstes bekannt geworden ist, auszufüllen und an die internen Kontaktpersonen zu übersenden.

Eine Einordnung, ob der Vorfall meldepflichtig im Sinne der DSGVO und/oder des BSI-Gesetzes ist, wird von den Kontaktpersonen auf Basis der Angaben im Meldebogen vorgenommen.

V. Wer sind die Kontaktpersonen, an die ein möglicher Vorfall intern zu melden ist?

Bitte informieren Sie im Falle eines möglichen Vorfalles unverzüglich:

- **[IT-Sicherheitsbeauftragte]**
- **[IT-Leiter]**
- **[DSB]**

VI. Interner Meldebogen

Bitte beachten:

- Der Meldebogen ist bei jeder Datenschutzverletzung und/oder jedem IT-Sicherheitsvorfall (nachfolgend gemeinsam: „Vorfall“) auszufüllen.
- Ziffern 1-4 sind von demjenigen Mitarbeiter auszufüllen, dem der Vorfall als erstes bekannt geworden ist. Dieser Mitarbeiter ist für den Versand des ausgefüllten Dokumentes an die Kontaktpersonen verantwortlich.
- Ziffern 5-12 sind von den Kontaktpersonen (ggf. unter Zuhilfenahme externer Beratung) auszufüllen. Eine Entscheidung, ob der Vorfall gemeldet wird, obliegt grundsätzlich der Geschäftsführung.
- Aufgrund der sehr kurzen Fristen (24h – 72h) ist zu gewährleisten, dass der ausgefüllte Meldebogen unverzüglich den Kontaktpersonen zugesendet wird, damit diese die Meldepflicht prüfen können und UNTERNEHMEN die gesetzlichen Pflichten einhalten kann.

Ziffern 1-5: Auszufüllen durch den Mitarbeiter
1. Zeitpunkt, in dem der Vorfall aufgetreten ist (*Bitte ausfüllen*)
2. Zeitpunkt der Kenntnisnahme von dem Vorfall (*Bitte ausfüllen*)
3. Beschreibung des konkreten Vorfalls
4.1 Art des Vorfalles (*Zutreffendes bitte ankreuzen und ggf. präzisieren*)
☐ Gezielter Angriff:
☐ Störung von Software-/Hardwarekomponenten:
☐ Datenschutzverletzung im Rahmen des Rechenzentrumsbetriebs:
☐ Verlust von Datenträgern:
☐ Diebstahl von Datenträgern:
☐ Irrtümliche/unrechtmäßige Übermittlung:
☐ Vorsatz/Fahrlässigkeit intern:
☐ Sonstige, und zwar:
4.2 Bereits ergriffene (technische und organisatorische) Maßnahmen, um den Schutz der betroffenen Datensätze zu gewährleisten (*Bitte ausfüllen*)
4.3 Kategorien der betroffenen Daten (*Zutreffendes bitte ankreuzen und ggf. präzisieren*)

Nicht personenbezogene Daten
☐ Betriebs- und Systemdaten (z. B. Konfigurationsdaten von IT-Systemen, Passwörter, Asset- und Inventardaten), und zwar:
☐ Produkt-, Forschungs- und Entwicklungsdaten (z. B. Konstruktionspläne, Patentanträge und Forschungsdaten), und zwar:
☐ Produktionsprozessdaten (z. B. Maschinensteuerungsdaten, Fertigungsrezepturen und Prozessparameter), und zwar:
☐ Kundendaten, und zwar:
☐ Sonstige, und zwar:
Personenbezogene Daten
☐ Stammdaten (z. B. Name, Adressdaten, Kontaktinformationen)
☐ Rechnungsbezogene Daten (z. B. Kontonummer, IBAN, Bankinstitut Leistungen)
☐ Lohn- und Gehaltsdaten (von Beschäftigten)
☐ Gesundheitsdaten
☐ Kommunikationsdaten
☐ Passwörter
☐ Sonstige, und zwar:
4.4 Ungefähre Anzahl betroffener Datensätze *(Bitte ausfüllen)*
4.5 Kategorien von der Datenschutzverletzung betroffener Personen (*Zutreffendes bitte ankreuzen und ggf. präzisieren*)
☐ Geschäftskunden/Lieferanten

☐ Mitarbeiter
☐ Bewerber
☐ Sonstige, und zwar:
4.6 Ungefähre Anzahl betroffener Personen/Kunden (*Bitte ausfüllen*)
4.7 Beschreibung der wahrscheinlichen Folgen des Vorfalles (*Zutreffendes bitte ankreuzen und ggf. präzisieren*)
☐ Ausfall von Produktionssystemen
☐ Ausfall von IT-Systemen
☐ Abfluss von Daten
☐ Kenntnisnahme von Daten durch unbefugte Dritte
☐ Kenntnisnahme durch unbefugte Dritte über persönliche Verhältnisse einer Person (z. B. Identitätsdiebstahl, Diskriminierung, Rufschädigung, finanzielle Nachteile, Offenbaren von Gesundheitsdaten):
☐ (Potenzieller) unbefugter Zugriff auf IT-Systeme von UNTERNEHMEN
☐ (Potenzieller) Immaterieller Schaden zu Lasten einer Person (z. B. Rufschädigung):
☐ Sonstige, und zwar:
4.8 Liegt eine grenzüberschreitende Datenschutzverletzung vor?
☐ Ja ☐ Nein
<u>Ziffern 5.-12: Auszufüllen durch die Kontaktpersonen</u>

5. Beschreibung der bereits ergriffenen forensischen Maßnahmen zur Aufklärung des Vorfalls (*Bitte ausfüllen*)
6. Beschreibung der vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung des Vorfalles (*Bitte ausfüllen*)
7. Name, Position und Kontaktdaten der meldenden Person (*Bitte ausfüllen*)
8. Führt der Vorfall voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen? (vgl. Art. 33 DSGVO)
☐ Ja ☐ Nein Begründung für die Annahme eines voraussichtlichen Risikos für die Rechte und Freiheiten natürlicher Personen:
Wenn unter 8 „Ja“, dann Meldung an die zuständige Datenschutzaufsichtsbehörde!
9. Kann der Vorfall (i) schwerwiegende Betriebsstörungen für die Dienste von UNTERNEHMEN oder (ii) finanzielle Verluste für UNTERNEHMEN verursachen oder hat der Vorfall bereits solche Schäden verursacht? (vgl. §§ 32, 2 Nr. 11 a) BSI-Gesetz)
☐ Ja ☐ Nein Begründung für die Annahme eigener (potenzieller) schwerwiegender Betriebsstörungen oder (potenzieller) finanzieller Verluste:

Wenn unter 9 „Ja“, dann Meldung an das BSI!
10. Kann der Vorfall eine andere natürliche oder juristische Person durch erhebliche materielle oder immaterielle Schäden beeinträchtigen oder hat der Vorfall bereits solche Schäden verursacht? (vgl. §§ 32, 2 Nr. 11 b) BSI-Gesetz)
☐ Ja ☐ Nein Begründung für die Annahme (potenzieller) erhebliche materielle oder immaterielle Schäden für andere natürliche oder juristische Personen:
Wenn unter 10 „Ja“, dann Meldung dann Meldung an das BSI! Wenn unter 10 „Ja“ und die potenziell betroffene Person eine natürliche Person ist, dann Meldung an die zuständige Datenschutzaufsichtsbehörde!
11. Besteht trotz der getroffenen technischen und organisatorischen Maßnahmen zur Minimierung der Auswirkungen des Vorfalles ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen? (vgl. Art. 34 DSGVO)
☐ Ja ☐ Nein Begründung für die Annahme eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen trotz ergriffener Maßnahmen zur Minimierung der Auswirkungen des Vorfalles:
Wenn unter 11 „Ja“, dann Benachrichtigung sämtlicher von dem Vorfall betroffenen natürlichen Personen!
12. Weitere sachdienliche Angaben

B. Übersicht über die Pflichten zur Meldung von Datenschutzverletzungen und/oder IT-Sicherheitsvorfällen[21]

I. Welche Vorfälle müssen binnen welcher Frist die zuständigen Behörden gemeldet werden?[22]

1. Erhebliche Sicherheitsvorfälle (BSI-Gesetz)

a) Meldung an das BSI

	Meldepflicht	Bis wann
1	**Unverzügliche Erstmeldung** bei erheblichen Sicherheitsvorfällen (vgl. § 32 Abs. 1 Nr. 1 BSI-Gesetz) Erheblich ist ein Sicherheitsvorfall, wenn Frage 9 und/oder 10 im internen Meldebogen mit „Ja“ beantwortet wird (vgl. §§ 32, 2 Nr. 11 BSI-Gesetz)	**Unverzüglich**, spätestens aber **innerhalb von 24h nach Kenntniserlangung**
2	**Erneute Meldung** über den erheblichen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden, inklusive einer ersten Bewertung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen; ggf. Kompromittierungsindikatoren angeben (vgl. § 32 Abs. 1 Nr. 2 BSI-Gesetz)	**Unverzüglich**, spätestens aber **innerhalb von 72h nach Kenntniserlangung**
3	Zwischenmeldungen auf Nachfrage des BSI (vgl. § 32 Abs. 1 Nr. 3 BSI-Gesetz)	Jederzeit
4	**Abschlussmeldung** mit einer ausführlichen Beschreibung des Sicherheitsvorfalls sowie Angaben zu Ursachen, Maßnahmen, grenzüberschreitenden Auswirkungen; dauert der Vorfall nach einem Monat noch an, erfolgt eine Fortschrittsmeldung (vgl. § 32 Abs. 1 Nr. 4 BSI-Gesetz)	**Innerhalb eines Monats** nach Übermittlung der Meldung des Sicherheitsvorfalls
5	Ist in Schritt 4 eine Fortschrittsmeldung anstelle einer Abschlussmeldung erfolgt, muss nach Abschluss der Bearbeitung des Sicherheitsvorfalls eine Abschlussmeldung erfolgen (vgl. § 32 Abs. 2 BSI-Gesetz).	**Innerhalb eines Monats** nach Abschluss der Bearbeitung des Sicherheitsvorfalls

[21] Dieser Teil B. richtet sich an die für Datenschutz und IT-Sicherheit verantwortlichen Mitarbeiter (Kontaktpersonen) und an die Geschäftsführung.

[22] Unter Umständen ist derselbe Vorfall sowohl gegenüber der Datenschutzaufsichtsbehörde, als auch gegenüber dem BSI zu melden.

b) Meldung an betroffene Kunden und Geschäftspartner

Das BSI kann bei erheblichen Sicherheitsvorfällen ein Unternehmen anweisen, die Empfänger ihrer Dienste (Kunden) zu unterrichten (vgl. § 35 BSI-Gesetz) (vgl. Ziffer 1).

Darüber hinaus kann – je nach Einzelfall – auch aus vertraglichen/nebenvertraglichen Pflichten seitens UNTERNEHMEN und/oder aus geschäftsstrategischen Gründen zur Vermeidung von Schäden eine Anzeige an die betroffenen Kunden/Geschäftspartner angezeigt sein. Ob eine solche Meldung erfolgt, ist einzelfallbezogen zu bewerten.

	Maßnahme	**Bis wann**
1	Auf Anweisung des BSI: Unterrichtung der Kunden und/oder Geschäftspartner („Empfänger ihrer Dienste"); ggf. durch Veröffentlichung im Internet, soweit dies sinnvoll ist.	Nach Anweisung unverzüglich
2	Je nach Einzelfall: Unterrichtung des Kunden wegen vertraglicher/nebenvertraglicher Pflichten und/oder aus geschäftsstrategischen Gründen.	Unverzüglich

2. Datenschutzverletzungen

Gemäß Art. 33 DSGVO heißt es:

„Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt."

Ob und wann die Verletzung „voraussichtlich nicht zu einem Risiko (…) führt", ist eine Rechtsfrage und anhand der Umstände des Einzelfalles zu bewerten.

Im Falle eines hohen Risikos sind zudem die Betroffenen zu benachrichtigen (vgl. Art. 34 DSGVO). Ob und wann ein solches „hohes Risiko" vorliegt, ist ebenfalls eine Rechtsfrage und anhand der Umstände des Einzelfalles zu bewerten.

Demnach gelten folgende Meldepflichten und Fristen:

	Risikograd	Maßnahme	Bis wann
1	Voraussichtlich kein Risiko für die Betroffenen	Dokumentationspflicht (Art. 5 Abs. 2 DSGVO)	Schnellstmöglich
2	Voraussichtliches Risiko für die Betroffenen	Dokumentationspflicht und Benachrichtigungspflicht gegenüber der Aufsichtsbehörde nach Kenntnis von dem Vorfall (vgl. Art. 33 DSGVO)	**Unverzüglich, möglichst innerhalb von 72 Stunden nach Kenntniserlangung**
3	Voraussichtlich hohes Risiko für die Betroffenen	Dokumentationspflicht, Benachrichtigungspflicht ggü. der Behörde und Benachrichtigungspflicht ggü. dem Betroffenen (Art. 34 DSGVO)	**Unverzüglich nach Kenntnis von dem Vorfall**

II. An welche Behörde muss wie gemeldet werden?

- Bei (meldepflichtigen) Datenschutzverletzungen:
  [Adresse zuständige Datenschutzaufsichtsbehörde]

  Meldungen werden über das Online-Portal eingereicht: https://datenschutz.hessen.de/service/meldung-nach-art-33-DSGVO.

- Bei (meldepflichtigen) IT-Sicherheitsvorfällen:

  BSI – Bundesamt für Sicherheit in der Informationstechnik
  Godesberger Allee 87
  53175 Bonn
  Telefon: +49 (0)228 99 9582-0
  Telefax: +49 (0)228 9910 9582-0
  E-Mail: bsi@bsi.bund.de

  Meldungen werden über das BSI-Portal eingereicht.

  Auf diesem muss man sich zunächst registrieren und anmelden: https://portal.bsi.bund.de/.

  Eine Anleitung zur Meldung von Vorfällen ist hier abrufbar: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Meldung/Anleitung-Meldung_node.html.