



Willi Plattes

Zukunft mit der Datenmacht des Mittelstands

Menschen und KI-Kompetenz

Readiness - Souveränität
Resilienz



PG

PLATTESGROUP

WILLI PLATTES

Zukunft mit der Datenmacht des Mittelstands

Menschen und KI-Kompetenz

Readiness · Souveränität · Resilienz

PLATTESGROUP

Reihe Familienvermögen

Geleitwort

Der deutsche Mittelstand hat viele Krisen gemeistert – Ölschocks, Finanzkrisen, Pandemie, Energiepreise. Er hat sie gemeistert, weil er etwas besitzt, das sich nicht in Bilanzen abbilden lässt: die Fähigkeit, Verantwortung nicht zu delegieren. Der Unternehmer, die Unternehmerin steht für den eigenen Betrieb ein – mit dem Namen an der Halle und oft genug mit dem eigenen Vermögen.

Genau diese Fähigkeit wird jetzt auf eine neue Probe gestellt. Die digitale Verwundbarkeit unserer Betriebe ist keine Randnotiz der IT-Abteilung mehr. Neun von zehn Opfern digitaler Erpressung sind kleine und mittlere Unternehmen – nicht die Konzerne, nicht „die anderen“. Und zugleich entscheidet sich in denselben Betrieben gerade die zweite große Frage dieses Jahrzehnts: ob der Mittelstand die Künstliche Intelligenz zu seinem Werkzeug macht – oder zu dem seiner Wettbewerber.

Ich weiß aus vielen Berichten mittelständischer Unternehmer, dass die erfolgreiche Implementierung von KI-Anwendungen Ihre Erwartungen in positiver Hinsicht übertroffen haben. Gleichwohl bleibt die Sorge vieler, in einem Themenfeld, das man bisher nur unzureichend kennt und beherrscht, unkalkulierbare Risiken einzugehen. Dieses Spannungsfeld zügig aufzulösen, wird gerade zu einer der Schlüsselfragen für die Wettbewerbsfähigkeit des Mittelstands.

Dieses Buch behandelt beide Fragen, also die Chancen und die Risiken der KI, als das, was sie sind: eine einzige Frage. Es erzählt – und das unterscheidet es von fast allem, was zu diesem Thema erschienen ist – die Geschichte eines Unternehmers, wie ich ihm in unseren Mitgliedsbetrieben täglich begegnen könnte: solide, digitalisiert, versichert, gut beraten. Und trotzdem verwundbar, weil niemand bemerkt hat, wie groß die Abhängigkeit geworden ist. Wer die Kapitel über den Morgen liest, an dem bei Thomas Hartmann die Bildschirme schwarz werden, legt das Buch anders wieder hin, als er es aufgenommen hat.

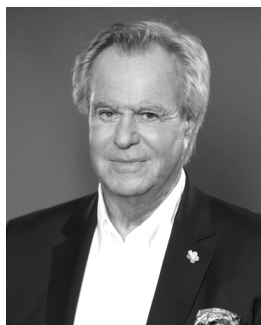
Vor allem aber macht dieses Buch keine Angst. Angst lähmt, und gelähmte Unternehmen investieren nicht. Es zeigt stattdessen, was Führung in dieser Lage bedeutet: die richtigen Fragen stellen, Nachweise verlangen, Routinen bauen – und dann den eigenen Datenschatz heben, der in vierzig Jahren Angeboten, Konstruktionen und Erfahrung liegt. Dass am Ende dieser Geschichte kein gerettetes, sondern ein produktiveres Unternehmen steht, ist die wichtigste Botschaft für unseren Standort.

Ich wünsche diesem Buch viele Leserinnen und Leser auf den Chefsesseln unseres Landes – und den Betrieben dahinter Führungskräfte, die seine Fragen nicht nur lesen, sondern in der nächsten Leitungssitzung stellen.

Senator a.D. Christoph Ahlhaus

Bundesgeschäftsführer des Bundesverbandes mittelständische Wirtschaft e.V.

Zum Autor



Willi Plattes ist verheiratet und hat fünf Kinder mit einer Frau. Ausbildung: Industriekaufmann; Betriebswirt (grad.); Diplom-Kaufmann; Bestellung zum deutschen Steuerberater in Nordrhein-Westfalen; spanischer Asesor Fiscal seit dem 25. April 2004 (Berufsregister Col·legiat Nr. 862).

Beruflicher Werdegang: Aufbau und Führung einer eigenen steuerberatenden Praxis in Deutschland mit bis zu 75 Mitarbeitern bis 1998. In diesem Jahr Auswanderung nach Spanien. Ab 2000 Aufbau der international tätigen Steuerberatungs- und Rechtsanwaltskanzlei PlattesGroup mit aktuell 110 Mitarbeitern (Stand August 2026); aktive Unternehmensbeteiligungen; Berufung in den Beirat der Commerzbank; Lehrbeauftragter an der Fachhochschule Köln; politische Tätigkeiten in der Stadt Frechen und im Landkreis.

Die PlattesGroup hat sich neben der steuerlichen und rechtlichen Beratung in Spanien insbesondere auf die Betreuung deutschsprachiger Kunden fokussiert. Hunderte deutschsprachige Unternehmen sind bei der Geschäftsgründung in Spanien begleitet worden und werden bis heute betreut. Zu den Mandanten zählen Familienbetriebe und Einzelunternehmer ebenso wie Family Offices, Versorgungsunternehmen und namhafte Aktiengesellschaften mit Börsennotierung im Ausland. Die Kanzlei betreut ein Immobilienvermögen von über acht Milliarden Euro.

Willi Plattes hat zahlreiche Veröffentlichungen zum Thema der Doppelbesteuerungsabkommen zwischen Spanien und Deutschland, Österreich und der Schweiz publiziert. Darüber hinaus erfolgen regelmäßige Publikationen über das spanische, deutsche und schweizerische Steuerrecht, insbesondere im Hinblick auf Ver-

knüpfungen zu EU-Staaten, Drittstaaten und Steueroasen. Als Referent ist er auf Veranstaltungen zum internationalen Steuerrecht tätig. Er ist zudem Initiator und Veranstalter des etablierten Events NEU DENKEN, das kurz vor seiner zehnten Ausgabe steht, sowie des Mandelblüten-Events.

Seit dem Durchbruch der generativen KI Anfang 2023 beschäftigt er sich intensiv mit Künstlicher Intelligenz. Im Haus sind daraus eigene Initiativen entstanden, in mehreren Bereichen ist KI bereits im Einsatz. Als familiengeführtes mittelständisches Unternehmen begleitet die Kanzlei ihre Mandanten auf diesem Weg aus eigener Erfahrung — für Willi Plattes ist das weniger ein Geschäftsfeld als eine Leidenschaft. Auch der Berufsstand der Rechts- und Steuerberatung wird von künstlicher Intelligenz unmittelbar verändert. Wer das ernst nimmt, muss sich von der Vorstellung verabschieden, dass irgendetwas so bleibt, wie es ist. Der Leitsatz, an dem sich die Arbeit im Haus ausrichtet: „Beständigkeit ist eine Illusion. Alles, was existiert, steht im Dienst des Wandels — nicht als Zeichen des Verlusts, sondern als Einladung zur Erneuerung.“

Inhalt

Geleitwort	2
Zum Autor	4
Inhalt	6
Prolog – Der Schatz und der schwarze Bildschirm	15
 Teil I – Den Datenschatz heben	 19
 1 Zukunft mit der Datenmacht des Mittelstands	 21
Zwei Meldungen an einem Dienstagmorgen.....	21
Der Abend bei Petersen	23
Was Hartmann besitzt, ohne es zu sehen	25
Das Sonntagessen	27
Die drei Fragen und die zentrale These	29
 2 Die Landkarte dieses Buches	 32
 Teil II – Wenn der Bildschirm schwarz wird	 37
 3 Der Anruf vor der Frühschicht	 39
Die Krise begann früher	46
 4 Wir sind doch kein Krankenhaus	 47
Der Irrtum, der vernünftig klingt	48
Digitalisierung: Leistung und Abhängigkeit.....	49
Der Kunde fragt früher als die Behörde.....	52
Der gefährliche Trost der Versicherung	54

Der Mensch ist kein Randthema.....	56
KI: Das neue Werkzeug ohne Inventarliste	57
Eine lästige Pflicht wird zum Verkaufsargument.....	60
Die erste ehrliche Bestandsaufnahme.....	61
Memo für die Geschäftsleitung.....	62
 5 Das macht doch unsere IT.....	65
Aufgabe und Verantwortung sind nicht dasselbe	65
Warum die IT allein nicht entscheiden kann.....	66
Der Protokollsatz, der später wehtut.....	67
Die Rolle des Geschäftsführers	68
Das erste Lagebild	69
Die Schulbank der Leitung	70
Was Hartmann ändert	70
 6 Es kommt keine Post vom Amt.....	72
Der falsche Trost der Unklarheit	72
Drei Prüfungen statt einer.....	73
Der Fragebogen als Warnsignal.....	75
Die Selbstprüfung darf nicht im Kopf bleiben	76
Der Irrtum der kleinen Gesellschaft	77
Keine Panikprüfung.....	78
Memo für die Geschäftsleitung.....	78

Teil III – Die neue Führungsaufgabe	81
7 Die zehn Fragen der Geschäftsleitung.....	83
Aus zehn Fragen wird ein Arbeitsplan.....	88
8 Der Mensch öffnet die Tür	91
Der Angriff auf die Hilfsbereitschaft	92
Schulduzuweisung vergrößert das Problem.....	92
Der Prozess war die Schwachstelle	93
Schulung ist kein Ereignis	94
Die Führung muss mitlernen	95
Den Überblick behalten.....	96
Vom Opfer zur Botschafterin	98
Der neue Zahlungsprozess.....	99
9 KI im Giftschränk	101
KI ist schon im Unternehmen	101
Halluzinationen: Ton sicher, Inhalt schwach.....	103
Daten hinein, Risiko heraus.....	104
Der Chatbot auf der Website	104
Die KI-Inventur	105
KI-Kompetenz ist Führungsaufgabe	106
Die ersten Regeln	106
10 Lieferkette: Die offene Seitentür	108
Unternehmensgrenze ist nicht Risikogrenze	108
Dienstleister sind keine Nebensache.....	109

Der Fernwartungszugang	110
Der Kunde als Prüfer	110
Sicherheit als Lieferfähigkeit	111
Die Lieferantenakte	112
Vertragsklauseln reichen nicht	112
Wenn Ihr Problem beim Kunden ankommt	113
 Teil IV – Die Folgen	 115
 11 Haftung: Aus Technik wird Verantwortung.....	 117
Ein Angriff ist nicht immer Ihr Verschulden	117
Erste Ebene: Schaden im Unternehmen	118
Zweite Ebene: Aufsicht und Bußgelder	119
Dritte Ebene: Beirat und Kontrolle	119
Vierte Ebene: Versicherung und Deckung	120
Fünfte Ebene: Verhalten nach dem Vorfall	121
Die Verteidigung heißt nicht Perfektion.....	121
Der Haftungsordner	122
 12 Wenn es brennt: Die ersten 72 Stunden	 124
Die erste Regel: nicht hektisch retten	124
Minute 1 bis 30: isolieren und dokumentieren	125
Der Krisenstab.....	125
Die erste Mitarbeiterinformation	126
Die Meldeuhren	127
Die Lösegeldfrage	128
Der zweite Schock: Datenabfluss	128

Der Wiederanlauf.....	129
Nach 72 Stunden	130
13 Gekauft ist nicht gedeckt	133
Eine Police ist kein Freibrief.....	133
Antrag gegen Wirklichkeit.....	134
Cyber-Police, D&O und Strafrechtsschutz.....	135
Obliegenheiten müssen in den Notfallplan.....	135
CEO-Fraud ist nicht automatisch Cyberdeckung	136
Die Versicherung als Hausaufgabenliste	137
Teil V – Die Ordnung.....	141
14 Das Cockpit: Nachweis statt Nervosität.....	143
Kein Berichtswesen für Bürokraten	143
Sechs Instrumente	144
Die Ampel muss ehrlich sein	145
Kennzahlen, die eine Geschäftsleitung versteht.....	146
Das offene Ticket	147
Nachweis ist Substanz	147
Der Rhythmus.....	148
Die Antwort an die Aufsicht.....	148
Memo für die Geschäftsleitung	149
15 Der Beirat auf dem Wachturm	150
Kontrolle braucht ein Lagebild	150
Der Beirat muss nicht technisch werden	151

Familienunternehmen und blinde Loyalität.....	151
Cyber und Nachfolge	152
Der Beiratsbericht	153
Zustimmungsvorbehalte und Budget	153
Der Wachturm	154
 16 Sonderfälle sind selten Auswege	156
Die Holding mit drei Leuten.....	156
Jede Gesellschaft, aber nicht isoliert.....	157
Die Krise als Verstärker	158
Finanzkunden und DORA-Druck	158
KRITIS und kritische Kunden	159
Ausland ist keine Abkürzung.....	159
Der Sonderfall darf nicht lähmen	160
 17 Vom Weckruf zur Gewohnheit	162
Vom Projekt zum Rhythmus.....	162
Die vier Routinen.....	163
Die Rolle der CyberPedia	163
Kultur schlägt Aktionismus	164
Der Weckruf darf nicht verklingen	165
 Teil VI – Der gehobene Schatz	167
 18 Der Anruf am Vormittag.....	169
Der Stammtisch.....	171
Diesmal kommt kein Erpresser	172

19 Die Schatzkarte.....	174
Die Ernüchterung	175
Die Auswahl.....	176
 20 Vierzig Minuten, richtig gemacht	 179
Der erste Anlauf scheitert.....	179
Der Regelbetrieb	180
Was im Cockpit ankam.....	181
 21 Gefunden werden	 183
Der Beirat dreht die Frage	184
Der Kreis schließt sich.....	185
 Epilog – Der ruhige Dienstag.....	 188
Gute Vorsorge hat selten Applaus	188
Was Hartmann gelernt hat	189
Was Unternehmer übergeben.....	190
Die emotionale Rendite	191
Der ruhige Dienstag ist kein Zufall	191
Schluss	192
 Das Führungsfragen-Register	 193
Ready – Wissen wir, wo wir stehen?	194
Souverän – Führen wir im Ernstfall?	196
Widerstandsfähig – Stecken wir das weg?	198
Compliant – Können wir es belegen?.....	200
Zukunftsfähig – Arbeitet unser Schatz?.....	202

Teil VII – Anhang	205
Anhang A Recht und Nachweis	206
Organhaftung – Das Unternehmen als Kläger	207
NIS-2, Leitungspflicht und § 38 BSIG.....	210
Schulungspflichten – Lernen muss belegbar sein.....	213
Lieferketten-Durchreichung – Neue Pflichten.....	216
DSGVO im Cybervorfall – 72-Stunden-Meldung.....	219
Cyber-Police – Antrag und Wirklichkeit.....	222
D&O-Versicherung – Persönliche Haftung	225
CEO-Fraud – Der Angriff auf den Menschen	227
EU AI Act – KI-Kompetenz und Transparenz.....	230
Lösegeld zahlen? – Der Graubereich.....	233
DORA – Die Finanzkunden-Kette.....	236
Nachweis – ISO 27001, BSIG, Auditfähigkeit	239
Beirat – Aufsichtspflicht und Haftung.....	242
Anhang B Zahlen, Fälle, Quellen	245
KPMG Global AI Pulse – Vier Zahlen zur Führungsfrage	246
Europe 2031 – Ein Szenario zur Führungsfrage	249
Befunde der Bitkom-Research.....	254
Die Rechnung: Was Cyberangriffe kosten	267
Was die Zahlen für die Führung bedeuten	276
CyberPedia als digitales Nachschlagewerk.....	277
Quellen	279

Danksagung.....	281
Abkürzungen.....	282
Glossar	285
Stichwortverzeichnis.....	287
Nutzungshinweise und Impressum	291

Prolog – Der Schatz und der schwarze Bildschirm

An einem Freitagabend im Frühjahr steht Thomas Hartmann allein in seiner Halle.

Die Frühschicht ist lange gegangen, die Spätschicht auch. Nur die Notbeleuchtung brennt. Es riecht nach Kühlschmierstoff und warmem Metall, und wenn man ganz still ist, hört man das leise Ticken einer Maschine, die abkühlt.

Hartmann macht das manchmal. Freitags, wenn die Woche vorbei ist, geht er einmal durch die Halle. Nicht um zu kontrollieren. Um zu sehen, was da ist.

Da ist viel.

Die Fräszentren, in die sein Vater investiert hat. Die Messmaschine, um die ihn Wettbewerber beneiden. Ganz vorne, im Eingangsbereich, die alte Fräsmaschine seines Großvaters, mit der alles begann. Drei Generationen, zum Anfassen.

Über Generationen lag der Wert des deutschen Mittelstands in genau solchen Dingen: in Maschinen, Hallen, Produkten, in der ruhigen Hand eines Meisters. Das gilt bis heute.

Aber daneben ist, fast unbemerkt, ein zweites Vermögen gewachsen. Akte für Akte, Vorgang für Vorgang. Es liegt nicht in der Halle. Es liegt in den Daten: in Konstruktionen und Kalkulationen, in Kundenbeziehungen und Fristen, in Erfahrungen und Entscheidungen. In allem, was ein Haus über Jahre gelernt hat – und was kein Programm aus dem Internet einfach besitzt.

Dieses zweite Vermögen kann man nicht anfassen. Man sieht es nicht, wenn man abends durch die Halle geht. Vielleicht ist es deshalb so lange niemandem aufgefallen.

Und lange arbeitete dieser Schatz nicht. Er lag in Ordnern, Postfächern und Köpfen. Er half dem Einzelnen, der wusste, wo etwas liegt. Der Organisation half er kaum.

Künstliche Intelligenz ändert das zum ersten Mal grundlegend. Sie hebt, was verborgen war. Sie findet, ordnet, verbindet, bereitet vor. Wer seine eigenen Daten produktiv macht, wird schneller, genauer, näher am Kunden. Das ist die große Chance dieses Jahrzehnts – und sie gehört nicht den Konzernen allein. Sie gehört gerade dem Mittelstand.

Doch jede Kraft hat eine Kehrseite.

Was produktiv wird, wird kritisch. Was ein Unternehmen trägt, kann es auch zu Fall bringen. Je tiefer Daten und KI in den Betrieb hineinwachsen, desto größer wird der Schaden, wenn der Zugang zu ihnen plötzlich fehlt.

Dann bleibt nur ein schwarzer Bildschirm. Weißer Text auf dunklem Grund. Eine Frist. Ein Betrag. Und ein Unternehmen, das von einer Minute auf die andere nicht mehr weiß, was es weiß.

Das ist keine ferne Drohung. Neun von zehn Opfern digitaler Erpressung sind kleine und mittlere Unternehmen. Nicht die Konzerne, nicht die Krankenhäuser, nicht „die anderen“. Es trifft Betriebe, die digitalisiert, investiert, sich versichert und ihrer IT vertraut haben. Nicht, weil sie nichts getan haben. Sondern weil niemand bemerkt hat, wie groß ihre Abhängigkeit inzwischen geworden ist.

Zwischen dem Schatz und dem schwarzen Bildschirm liegt ein schmaler Grat. Und was darüber entscheidet, auf welche Seite ein Unternehmen fällt, ist am Ende keine Frage der Technik.

Es ist eine Frage der Führung.

Eine Firewall kann man kaufen. Eine Police kann man abschließen. Einen Dienstleister kann man beauftragen. Aber die Entscheidung, was ein Unternehmen mit seinen Daten tut – wie es sie nutzt, schützt und verantwortet –, lässt sich nicht delegieren. Sie bleibt oben. Sie bleibt Chefsache.

Von dieser Entscheidung handelt dieses Buch. Es feiert die KI nicht blind, und es will keine Angst machen; Angst verkauft schnell, aber sie führt schlecht. Es zeigt einen anderen Weg: wie ein Unternehmer die Chance ergreift, ohne die Kontrolle zu verlieren. Wie aus

einem technischen Thema eine Führungsroutine wird. Und wie jemand mit auf die Kommandobrücke tritt, der die gefährlichen Gewässer kennt – ein Lotse, ein Schutzengel –, während das Kommando dort bleibt, wo es hingehört: bei Ihnen.

Der Mann in der Halle weiß an diesem Freitagabend noch nichts von alledem.

Er sieht seine Maschinen. Er sieht nicht seinen Schatz. Und er ahnt nicht, dass in einigen Wochen ein Telefon klingeln wird. Um 05:17 Uhr, elf Minuten vor dem Wecker. Sie werden ihn dann durch dieselbe Halle begleiten, hell erleuchtet und voller schweigender Maschinen, und sehen, wie schnell aus Stärke Ohnmacht werden kann.

Aber noch ist nicht 05:17 Uhr.

Noch ist Zeit.

Diese Zeit ist dieses Buch.

Teil I – Den Datenschutz heben

Die Chance

1 | Zukunft mit der Datenmacht des Mittelstands

Es gibt Momente, in denen eine Branche nicht nur eine neue Nachricht produziert, sondern ihre Richtung ändert. Der Mai 2026 war ein solcher Moment.

Thomas Hartmann hat ihn beinahe verpasst.

Zwei Meldungen an einem Dienstagmorgen

Es war ein Dienstag, kurz vor sieben. Hartmann saß in seinem Büro über der ersten Tasse Kaffee und ging die Wirtschaftsnachrichten durch, wie jeden Morgen: Energiepreise, Tarifabschluss, ein Kommentar zur Konjunktur. Dazwischen zwei Meldungen aus der KI-Welt.

Anthropic, eines der mächtigsten KI-Häuser der Welt, hatte gemeinsam mit Blackstone, Hellman & Friedman und Goldman Sachs eine neue, rund anderthalb Milliarden US-Dollar schwere Gesellschaft angekündigt. Ihr Zweck: Unternehmen dabei zu helfen, das KI-System Claude tief in ihre operativen Abläufe einzubetten – ausdrücklich mit Blick auf mittelständische und von Finanzinvestoren gehaltene Unternehmen. Wenige Tage später stellte OpenAI die OpenAI Deployment Company vor: getragen von rund zwanzig großen Investoren und Umsetzungspartnern, angeführt von TPG, mit mehr als vier Milliarden US-Dollar Anfangskapital. Den Kern bildete die Übernahme eines Londoner Beratungshauses mit rund hundertfünfzig sogenannten Forward Deployed Engineers – Menschen, deren Beruf es ist, KI nicht bereitzustellen, sondern in Unternehmen hineinzutragen.

Hartmann überflog beide Meldungen in vierzig Sekunden.

Große Namen, große Summen, große Erwartungen. So liest sich seit Jahren fast jede Nachricht aus dieser Welt. Er dachte: Milliarden. Amerika. Konzerne. Er dachte, ehrlich gesagt, gar nichts weiter. Er legte das Tablet wieder auf den Schreibtisch und ging in die

Produktionsbesprechung. Um acht hatte er einen Liefertermin zu retten, um zehn ein Bankgespräch.

So lesen die meisten Unternehmer solche Meldungen. In diesem Fall ein Fehler.

Denn man konnte diese beiden Nachrichten auch anders lesen: als öffentliches Eingeständnis.

Die führenden KI-Labore der Welt haben in jenen Maitagen sichtbar gemacht, dass ihr Rennen nicht mehr allein auf der Ebene der Modelle entschieden wird. Nicht mehr nur: Wer hat das leistungsfähigste Sprachmodell, die besten Benchmarks, die beeindruckendste Demo? Das alles bleibt wichtig. Aber es ist nicht mehr das Entscheidende.

Das Entscheidende beginnt dort, wo Unternehmen wirklich arbeiten. In ihren Daten. In ihren Prozessen. In ihren Fristen, ihrer Produktion, ihrer Beratung, ihrer Kommunikation mit Kunden, Banken, Lieferanten und Behörden.

Die großen KI-Häuser haben verstanden: Wer nur ein Modell verkauft, bleibt austauschbar. Wer aber in die Organisation des Kunden hineingeht, Datenräume erschließt, Arbeitsabläufe umbaut, Mitarbeiter befähigt und KI so tief in die Wertschöpfung integriert, dass sie Teil des Betriebs wird, gewinnt eine ganz andere Stellung.

Das ist kein Softwareverkauf mehr. Das ist Organisationsumbau.

Deshalb schicken diese Häuser nicht mehr nur Zugangsdaten. Sie schicken Menschen.

Und deshalb betrifft diese Entwicklung nicht nur Konzerne, Private-Equity-Portfolios und globale Banken. Sie betrifft Maschinenbauer wie Hartmann. Sie betrifft Händler und Dienstleister, Landwirtschaftsbetriebe und Family Offices, Hidden Champions und Startups – jeden Betrieb, dessen Wert nicht nur in Maschinen, Gebäuden oder Kapital liegt, sondern auch in Wissen.

Der eigentliche Wettbewerb der nächsten Jahre wird nicht in den Rechenzentren von San Francisco entschieden.

Er wird im Maschinenraum entschieden. Auch in dem von Thomas Hartmann.

Nur wusste der das an diesem Dienstag noch nicht.

Der Abend bei Petersen

Drei Wochen später saß Hartmann beim Unternehmerabend der Region. Kalte Platten, warmes Bier, vertraute Gesichter. Man sprach über Fachkräfte, über Energiekosten, über den Flächennutzungsplan.

Dann sprach Petersen.

Petersen war Mitte dreißig, führte in zweiter Generation ein Unternehmen für Gebäudetechnik, hundertzwanzig Mitarbeiter, und galt am Tisch als der Junge, der immer etwas Neues hatte. An diesem Abend hatte er etwas Neues.

„Bei uns sitzen seit sechs Wochen zwei Leute von einem KI-Haus im Büro“, sagte er. „Die bauen nichts Neues. Die nehmen, was wir haben. Zwanzig Jahre Wartungsprotokolle, Angebote, Aufmäße, Reklamationen. Die sagen, das ist unser Kapital. Wir merken es nur nicht, weil es in vierzig Ordnern liegt.“

Jemand fragte, was das kostete.

Petersen nannte eine Zahl. Am Tisch wurde gelacht, halb anerkennend, halb abwehrend.

„Und was bringt es?“, fragte Hartmann.

„Ein Beispiel“, sagte Petersen. „Ein Servicetechniker steht vor einer Anlage, die spinnt. Früher hat er den Kollegen angerufen, der die Anlage kennt. Wenn der Urlaub hatte, hat er gesucht. Heute fragt er ein System, das alle unsere Protokolle kennt, und bekommt in einer Minute die drei wahrscheinlichsten Ursachen – mit dem Hinweis, wann wir genau diesen Fehler schon einmal hatten und was damals geholfen hat. Aus unseren eigenen Unterlagen. Nicht aus dem Internet.“

Einen Moment war es still am Tisch.

„Und wisst ihr, was mir die beiden erzählt haben, als ich gefragt habe, warum sie ausgerechnet zu uns kommen?“, fuhr Petersen fort. „Die haben gesagt: Schauen Sie sich an, was gerade passiert. OpenAI und Anthropic haben in diesem Frühjahr Milliarden eingesammelt – nicht für neue Modelle, sondern für Gesellschaften, deren einziger Zweck es ist, KI in Unternehmen hineinzutragen. Mit eigenen Leuten, die vor Ort die Abläufe umbauen. Die fangen bei den Konzernen und den großen Beteiligungsgesellschaften an, weil da die großen Verträge liegen. Aber das Geschäftsmodell lebt von Skalierung. Was die bei den Großen lernen, verpacken sie in Standardbausteine – und dann kommen sie in den Mittelstand. Nicht vielleicht. Planmäßig. Die Frage ist nicht, ob diese Welle uns erreicht. Die Frage ist nur, ob wir dann etwas Geordnetes haben, worauf sie treffen kann – oder ob wir bei null anfangen, während der Wettbewerber schon zwei Jahre Vorsprung hat.“

„Das sagen Leute, die dir genau das verkaufen“, warf jemand ein.

„Ja“, sagte Petersen ruhig. „Hab ich denen auch gesagt. Wisst ihr, was die geantwortet haben? ‚Stimmt. Und der Dachdecker, der Ihnen sagt, dass Ihr Dach undicht ist, verdient auch an der Reparatur. Deswegen regnet es trotzdem rein.‘“

Hartmann musste an die beiden Meldungen denken, die er vor drei Wochen am Dienstagmorgen überflogen hatte. Milliarden. Amerika. Konzerne. Er hatte sie in vierzig Sekunden abgehakt.

Jetzt saßen die vierzig Sekunden mit am Tisch.

Dann sagte Hartmann den Satz, an den er sich später noch oft erinnern sollte.

„Das ist etwas für Konzerne, Petersen. Oder für Leute mit Zeit. Wir haben volle Auftragsbücher und keine zwei Mann übrig, die monatelang Ordner sortieren.“

Ein vernünftiger Satz, der nach Bodenhaftung klang. Nach einem Unternehmer, der sich nicht von jeder Mode treiben lässt. Die Hälfte des Tisches nickte.

Merken Sie sich diesen Satz. Er ist der Zwillingbruder eines anderen Satzes, der später in diesem Buch fallen wird und der genauso vernünftig klingt: „Wir sind doch kein Krankenhaus.“

Beide Sätze fühlen sich im Moment des Aussprechens wie gesunder Menschenverstand an.

Der eine Satz schiebt ein Risiko weg. Der andere schiebt eine Chance weg.

Beide sind Führungsentscheidungen, die als Randbemerkung getarnt sind.

Was Hartmann besitzt, ohne es zu sehen

Auf der Heimfahrt an diesem Abend ließ Petersens Beispiel Hartmann nicht los. Nicht, weil er es glaubte. Sondern weil es ihn irgendwie ärgerte.

Am Samstagvormittag darauf – das Werk war still, nur der Versand arbeitete eine halbe Schicht – ging er hinüber ins Archiv. Er suchte nichts Bestimmtes. Er wollte nur einmal sehen, was da eigentlich lag.

Da lagen: die Angebotsordner seit 1987, sein Vater hatte auf Durchschriften bestanden. Die Konstruktionszeichnungen, erst auf Papier, dann auf Mikrofilm, dann digital. Wartungs- und Störungsberichte für Anlagen, die längst verschrottet waren – und für solche, die noch heute liefen. Reklamationsakten, in denen stand, welcher Werkstoff sich bei welchem Kunden in welcher Anwendung bewährt hatte und welcher nicht.

Und das war nur das Papier.

Im ERP lagen dreißig Jahre Aufträge, Preise, Liefertermine, Kalkulationen. In den E-Mail-Postfächern lag die halbe Verhandlungsgeschichte des Unternehmens. Und in den Köpfen – im Kopf von Keller, dem Produktionsleiter, im Kopf von Meister Brandt, der in vier Jahren in Rente gehen würde – lag das, was nirgendwo stand: warum Linie drei bei feuchtem Wetter anders klang, welcher

Kunde Zeichnungen dreimal änderte und trotzdem pünktlich beliefert werden wollte, welche Toleranz man bei welchem Material wirklich halten konnte.

Hartmann stand zwischen den Regalen und dachte zum ersten Mal einen Gedanken, der ihm fremd vorkam:

Das hier weiß niemand außer uns.

Genau das ist der Schatz. Nicht als Metapher. Als Bestandsaufnahme.

Ein Maschinenbauer besitzt Produktionsdaten, Stücklisten, Konstruktionsunterlagen, Wartungshistorien, Qualitätsprüfungen, Reklamationsmuster und Erfahrungswerte aus Jahrzehnten.

Ein Medizintechnikhersteller besitzt Entwicklungsdokumentationen, Validierungsprozesse und die Erfahrung, welche Lösungen sich im klinischen Alltag bewähren und gleichzeitig geltende Gesetze einhalten.

Ein Logistikunternehmen verfügt über Tourenwissen, Kapazitätsdaten, Prozessabläufe und besondere Kenntnisse darüber, wie Lieferketten auch unter schwierigen Bedingungen stabil gehalten werden.

Ein Händler besitzt Kundenbeziehungen, Sortimentswissen, Einkaufs- und Preisdaten, Absatzhistorien sowie eine gute Vorstellung davon, welche Produkte, Angebote und Beratungsansätze sich in unterschiedlichen Markt- und Kundensituationen bewähren.

Ein Family Office besitzt Beteiligungsstrukturen, Familienlogiken und hochsensible Entscheidungsgrundlagen.

Ein Vermögensverwalter besitzt Risikoprofile und die Erfahrung, wie sich Menschen in guten und in schlechten Marktphasen verhalten.

Jedes dieser Häuser besitzt Wissen, das in keinem Lehrbuch steht und in keiner öffentlichen Datenbank abgebildet ist.

Ein allgemeines KI-Modell kann einen Text über Wartung schreiben. Aber es kennt nicht Linie drei der Hartmann Maschinenbau GmbH. Es kennt nicht die Störungshistorie, die Ersatzteillage, den

Liefertermin und die wirtschaftliche Folge eines Ausfalls. Es kann eine Vertragsklausel erklären. Aber es kennt nicht die Verhandlungsgeschichte, die steuerlichen Nebenwirkungen und die Frage, ob die elegante Lösung in der Praxis hält.

Die allgemeine Antwort wird in den nächsten Jahren immer billiger.

Die präzise, quellenbasierte, kontextbezogene, haftungsfeste Antwort wird immer wertvoller.

Und die entsteht nur dort, wo eigenes Wissen liegt.

Das ist der Vorteil des Mittelstands – der einzige, der ihm im KI-Zeitalter niemand streitig machen kann. Weniger Kapital als die Plattformen, weniger Rechenleistung, mehr Regulierung: alles wahr. Aber Nähe zum echten Problem, Tiefe in der Nische, Jahrzehnte an Domänenwissen – das haben die Plattformen nicht.

Europa hat das Rennen um die größten allgemeinen Sprachmodelle, die Large Language Models (LLM), nicht gewonnen. Diese Feststellung ist unbequem, aber notwendig. Nur führt sie oft zum falschen Schluss. Der Mittelstand muss nicht das nächste OpenAI werden. Hidden Champions müssen keine Grundlagenmodelle bauen. Der Kampfplatz ist ein anderer: der eigene Maschinenraum. Die Frage ist nicht, wer das beste Modell baut. Die Frage ist, wer seine eigenen Daten so ordnet, dass ein Modell darauf verlässlich arbeiten kann.

Hartmann schloss an diesem Samstag das Archiv ab und fuhr nach Hause. Er hatte den Schatz gesehen.

Was er in diesem Moment noch nicht gesehen und verstanden hatte: dass ein Schatz, den man hebt, bewacht werden muss.

Das Sonntagessen

Am nächsten Tag saß die Familie am Tisch. Es gab Braten, es gab die üblichen Themen, und irgendwann erzählte Thomas Hartmann von Petersen und von seinem Samstag im Archiv. Er erzählte es amüsiert, als Anekdote.

Seine Schwester Carola hörte zu, wie sie immer zuhörte: ruhig, mit diesem Blick, der Bilanzen lesen konnte. Carola führte den Beirat der Familiengruppe. Sie stellte selten viele Fragen. Sie stellte die eine.

„Angenommen, Petersen hat recht“, sagte sie, „und euer Archiv ist bares Geld wert. Wer kann da eigentlich alles ran?“

Thomas lachte. „An unser Archiv? Da will keiner ran, Carola. Das sind vierzig Jahre Staub.“

„Du hast gerade eine halbe Stunde erklärt, dass es kein Staub ist. Dass es das Einzige ist, was euch keiner nachmachen kann.“ Sie legte das Besteck ab. „Dann frage ich noch mal: Wer kann da ran? Wer könnte es kopieren? Wer könnte es euch wegnehmen – oder einfach nur abschließen, sodass ihr selbst nicht mehr rankommt?“

Hartmann wollte antworten und merkte, dass er die Antwort nicht kannte.

„Das müsste ich Baumann fragen“, sagte er.

„Ja“, sagte Carola. „Das dachte ich mir.“

Es blieb an diesem Sonntag bei dieser einen Szene. Kein Streit, kein Drama, der Braten wurde kalt, das Gespräch ging weiter. Aber die Frage blieb im Raum stehen, und sie ist die Frage, um die sich der Rest dieses Buches dreht.

Denn hier liegt der Denkfehler fast aller KI-Diskussionen im Mittelstand: Chance und Schutz werden als zwei Themen behandelt. Erst Innovation, später Sicherheit. Erst der Chatbot, später die Governance. Erst Produktivität, danach Risikomanagement. Zwei Projekte, zwei Budgets, zwei Zuständigkeiten.

In Wahrheit ist es ein einziges Thema.

Wissen, das nur in Köpfen liegt, skaliert nicht. Wissen, das in Postfächern verschwindet, ist schwer auffindbar. Wissen, das in PDFs abgelegt, aber nicht strukturiert ist, bleibt träge. Wissen, das nicht qualitätsgesichert ist, kann durch KI sogar gefährlicher werden, weil KI auch aus schlechten Daten überzeugende Sätze macht.

Und Wissen, das nicht geschützt ist, wird genau in dem Moment zum Risiko, in dem man es produktiv macht.

Solange der Schatz in den Archiven schlummert, interessiert er niemanden. Sobald er gehoben ist – auffindbar, verbunden, in Prozesse eingebaut, jeden Tag im Einsatz –, ist er zweierlei zugleich: das wertvollste Kapital des Unternehmens und sein verwundbarster Punkt.

Was produktiv wird, wird kritisch.

Dieser Satz ist die Achse dieses Buches. Alles Weitere folgt aus ihm.

Die drei Fragen und die zentrale These

Aus alledem ergeben sich drei Fragen, die sich jede Geschäftsleitung stellen sollte – nicht irgendwann, sondern in diesem Jahr.

Die erste Frage lautet: Welches Wissen besitzen wir, das ein allgemeines KI-Modell nicht hat? Wenn die Antwort lautet: nichts Wesentliches, dann ist das Unternehmen austauschbar, und ein KI-gestützter Wettbewerber wird die Leistung schrittweise nachbilden. Vielleicht nicht morgen. Aber früher, als vielen lieb ist. Wenn die Antwort lautet: jahrzehntelange Erfahrung, Spezialwissen, Prozessdaten, Kundennähe – dann beginnt die eigentliche Arbeit. Denn dann folgt sofort die Anschlussfrage: Ist dieses Wissen auffindbar, strukturiert, aktuell, qualitätsgesichert, rechtlich nutzbar – und geschützt?

Die zweite Frage lautet: Wie tief sind wir in die operativen Abläufe unserer Kunden eingebunden? Wer nur austauschbare Einzelleistungen liefert, ist leichter ersetzbar. Wer in Fristen, Datenflüsse und Entscheidungsprozesse seiner Kunden eingebunden ist, wird schwerer austauschbar. Das gilt für Industrie, Beratung und Vermögensstrukturen gleichermaßen. Und es bekommt eine neue Dimension: Die künftigen Auftraggeber sind immer häufiger nicht mehr nur Menschen, sondern deren KI-Systeme – Einkaufssysteme, die Lieferanten vorselektieren, Assistenten, die Berater vorschlagen, Prüfroutinen, die Nachweise maschinell lesen. Diese Systeme reagieren nicht auf guten Ruf und schöne Broschüren. Sie

reagieren auf strukturierte Information, auf Quellen, auf belegbare Qualität. Wer für sie nicht auffindbar ist, schafft es kaum noch in die Vorauswahl.

Die dritte Frage lautet: Sind wir KI-fähig und sicherheitsfähig zugleich? KI-fähig ist ein Unternehmen, das seine Daten, sein Wissen und seine Prozesse so strukturieren kann, dass KI daraus messbaren Nutzen erzeugt. Sicherheitsfähig ist es, wenn dabei Vertraulichkeit, Integrität, Verfügbarkeit, Zugriffskontrolle und Nachweisführung erhalten bleiben. Erst beides zusammen ergibt Zukunftsfähigkeit.

Damit ist die zentrale These dieses Buches ausgesprochen: Unternehmen müssen KI einsetzen, um zukunftsfähig zu bleiben. Neben KI-Kompetenz und Readiness müssen sie gleichzeitig Cybersicherheit, Datenschutz, Daten-Governance, Resilienz und Souveränität aufbauen, damit diese KI-Nutzung nicht zur offenen Flanke wird.

Beides gehört zusammen. Nicht nacheinander. Nicht in getrennten Projekten.

Cybersicherheit ist dabei nicht die Bremse, als die sie oft behandelt wird – Schutzschild, Kostenstelle, notwendiges Übel. Sie ist die Voraussetzung. Ein Unternehmen, das seine Zugriffe nicht kennt, kann keine KI-Agenten verantworten. Ein Unternehmen, das seine Datenqualität nicht kennt, kann KI-Ergebnisse nicht bewerten. Ein Unternehmen, das seine Systeme nicht wiederherstellen kann, baut Produktivität auf Sand. Und ein Unternehmen, das nicht dokumentieren kann, worauf eine Entscheidung beruht, verliert in allen Branchen, in denen Vertrauen Teil des Produkts ist – Vermögensverwaltung, Medizin, regulierte Industrie, Rechtsberatung –, den entscheidenden Vorteil: Nachvollziehbarkeit.

Souveränität heißt dabei nicht Abschottung und nicht nur nationale Cloud. Für ein Unternehmen heißt Souveränität zuerst: Es weiß, welche Daten es hat, wo sie liegen, wer darauf zugreifen darf, welche Systeme damit arbeiten – und was es im Ernstfall nachweisen kann. Souveränität ist ein Organisationszustand. Und Resilienz heißt nicht, dass nichts passiert. Resilienz heißt, dass ein Unternehmen nicht planlos wird, wenn etwas passiert.

Hartmann hätte an jenem Sonntag mit keinem dieser Begriffe etwas anfangen können.

Er hatte nur diese eine Frage seiner Schwester im Ohr, auf die er keine Antwort wusste.

Er nahm sich vor, am Montag mit IT-Leiter Baumann zu sprechen.

Dann kam der Montag, und mit ihm ein Reklamationsfall, ein krankgemeldeter Schichtführer und ein Liefertermin. Das Gespräch mit Baumann fand nicht statt.

So sterben die wichtigsten Fragen in Unternehmen: nicht an Widerspruch. An Dienstagen.

2 | Die Landkarte dieses Buches

Bevor wir Thomas Hartmann zu seinem schwersten Morgen begleiten, halten wir kurz an. Sie sollen wissen, wohin diese Reise geht und warum sie so aufgebaut ist, wie sie aufgebaut ist.

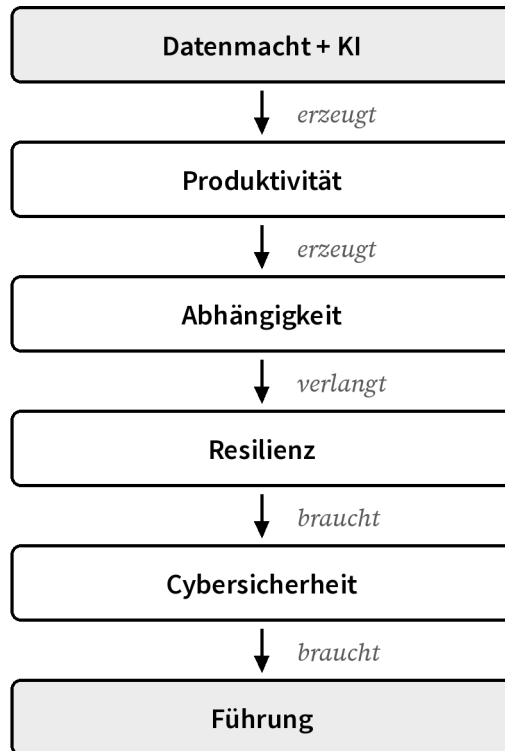
Die alte Frage an Unternehmen lautete: Sind unsere Prozesse digitalisiert?

Die neue Frage lautet: Sind unsere Prozesse KI- und sicherheitsfähig?

Dahinter steht eine Gleichung, die dieses Buch trägt und die Sie nach der Lektüre auswendig kennen werden:

Datenmacht plus KI erzeugt Produktivität. Produktivität erzeugt Abhängigkeit. Abhängigkeit verlangt Resilienz. Resilienz braucht Cybersicherheit. Cybersicherheit braucht Führung.

Die Gleichung dieses Buches



Jedes Glied dieser Kette ist ein Teil dieses Buches.

Das erste Kapitel hat die Chance beschrieben: den Schatz, den Hartmann in seinem Archiv gesehen hat, und die Bewegung der großen KI-Häuser hinein in die Maschinenräume des Mittelstands. Vielleicht haben Sie beim Lesen an Ihr eigenes Archiv gedacht, an Ihre Mandatsakten, Ihre Wartungshistorien, Ihre Kundengeschichte. Das war die Absicht.

Was jetzt kommt, ist der Stresstest.

Gleich klingelt ein Telefon. Um 05:17 Uhr, elf Minuten vor dem Wecker. Sie werden erleben, wie ein gut geführtes, profitables, digitalisiertes Unternehmen an einem einzigen Morgen die Kontrolle

über sein eigenes Wissen verliert – und warum in dieser Stunde nicht die IT gefragt ist, sondern die Spitze.

Man könnte fragen: Warum erzählt ein Buch über die Chancen der KI zuerst eine Katastrophe?

Aus einem einfachen Grund: Der schwarze Bildschirm ist die Kehrseite der neuen Produktivität. Je stärker ein Unternehmen seine Daten nutzt, desto größer wird der Schaden, wenn diese Daten nicht verfügbar, nicht vertrauenswürdig oder nicht geschützt sind. Wer den Maschinenraum produktiv machen will, muss wissen, was passiert, wenn er stillsteht. Der Anruf vor der Frühschicht ist deshalb keine Horrorgeschichte. Er ist die Rückseite von Kapitel 1.

Und noch etwas werden Sie sehen: Die Krise beginnt nicht um 05:17 Uhr. Um 05:17 Uhr wird sie nur sichtbar. Sie beginnt Monate vorher – in Sätzen, die vernünftig klingen. „Wir sind doch kein Krankenhaus.“ „Das macht unsere IT.“ „Es kommt schon Post vom Amt, wenn wir gemeint sind.“ Und, Sie erinnern sich an den Abend bei Petersen: „Das ist etwas für Konzerne.“

Deshalb rollen wir die Krise nach dem schwarzen Morgen rückwärts auf. Nicht technisch. Unternehmerisch. Wir fragen, welche Annahmen falsch waren, welche Entscheidungen fehlten, welche Nachweise nicht vorlagen, welche Menschen nicht vorbereitet waren, welche Versicherung nur scheinbar beruhigte und welche KI-Nutzung ungeordnet blieb.

Das Buch folgt dabei fünf Bewegungen.

Die Landkarte dieses Buches

Fünf Bewegungen – vom Weckruf zur Ernte



Dieselbe Halle: erst der Weckruf, dann die Ernte.

Zuerst die Chance: die Datenmacht des Mittelstands. Sie haben sie gerade gelesen.

Dann der Stresstest: der Anruf vor der Frühschicht und die Irrtümer, die ihn möglich machten.

Dann die neue Führungsaufgabe: die Fragen, die jede Geschäftsleitung stellen muss – zu Risiken, Menschen, KI-Werkzeugen und Lieferketten.

Dann die Ordnung: Haftung, die ersten 72 Stunden, Versicherung, Cockpit, Beirat – wie aus dem Weckruf eine Führungsroutine wird.

Und schließlich die Ernte: Wie derselbe Unternehmer, der beinahe alles verlor, seinen Schatz tatsächlich hebt – und warum ausgerechnet seine Sicherheitsarbeit dabei zum Wettbewerbsvorteil wird. Denn dieses Buch endet nicht mit einer überstandenen Krise. Es endet mit einem Unternehmen, das produktiver ist als vorher.

Thomas Hartmann steht dabei stellvertretend für viele. Er ist kein schlechter Unternehmer, und er ist nicht naiv. Er hat digitalisiert, investiert, modernisiert, eine Versicherung abgeschlossen und seiner IT vertraut. Gerade deshalb ist seine Geschichte wichtig: Viele Unternehmen werden nicht getroffen, weil sie nichts in dem Bereich getan haben. Sie werden getroffen, weil sie nicht gesehen haben, wie stark ihre Abhängigkeit dort gewachsen ist.

Die Hartmann Maschinenbau GmbH ist fiktiv. Thomas Hartmann ist fiktiv. Der Anruf, der jetzt kommt, ist es nicht. Solche Anrufe gibt es – in anderen Namen, anderen Hallen, anderen Branchen. Der Satz klingt fast immer gleich: „Wir kommen nicht rein.“

Es ist Nacht geworden über der Halle, durch die Hartmann am Anfang dieses Buches gegangen ist.

In elf Minuten klingelt der Wecker.

Das Telefon ist schneller.

Teil II – Wenn der Bildschirm schwarz wird

Der Stresstest – warum beruhigende Sätze gefährlich werden

3 | Der Anruf vor der Frühschicht

Um 05:17 Uhr klingelte das Telefon. Nicht der Wecker. Der hätte noch elf Minuten gehabt.

Thomas Hartmann wusste das sofort, noch bevor er richtig wach war. Es gibt Geräusche, die gehören zum Leben eines Unternehmers. Das Tor der Halle am frühen Morgen. Das erste Anlaufen einer Maschine. Das kurze Klacken eines Kugelschreibers vor einer schwierigen Unterschrift. Das Telefon um diese Uhrzeit gehört nicht dazu.

Auf dem Display stand:

Keller Produktion.

Hartmann setzte sich auf. Neben ihm wurde seine Frau wach, nicht ganz, nur so weit, wie Menschen wach werden, wenn sie spüren, dass etwas im Raum nicht stimmt.

| „Thomas?“

Er hob die Hand. Nicht jetzt.

| „Hartmann.“

Am anderen Ende war es laut und leise zugleich. Stimmen im Hintergrund. Schritte. Ein metallisches Geräusch. Aber nicht das vertraute Brummen einer Halle, die in den Tag findet.

| „Herr Hartmann, entschuldigen Sie die Uhrzeit“, sagte Keller.
| „Wir kommen nicht rein.“

Hartmann stand auf. Der Fliesenboden war kalt.

| „Wo nicht rein?“

| „Ins ERP. Arbeitsvorbereitung auch nicht. Versand auch nicht.
| Leitstand auch nicht.“

Hartmann ging zum Fenster. Draußen war es noch dunkel. Zwei Häuser weiter brannte bereits Licht in der Bäckerei. Irgendwo begann ein normaler Arbeitstag.

| „Was sehen Sie?“

Keller schwieg. Dieses Schweigen war der erste Bericht des Tages.

„Sagen Sie es.“

„Auf den Bildschirmen steht überall dasselbe. Ihre Daten wurden verschlüsselt. Wir sollen zahlen. In Bitcoin. Da ist eine Frist.“

Hartmann schloss kurz die Augen. Hartmann Maschinenbau GmbH. Dritte Generation. Hundertachtzig Mitarbeiter. Zulieferer für mehrere große Industriekunden. Eine Fertigung, die auf Takt, Präzision und Verlässlichkeit gebaut war. Sein Großvater hatte mit einer Fräsmaschine angefangen, die heute im Eingangsbereich stand. Sein Vater hatte Lieferketten aufgebaut. Thomas Hartmann hatte das Unternehmen digitalisiert: Cloud-ERP, vernetzte Fertigung, Scanner im Versand, digitale Arbeitsvorbereitung, internationale Angebotsprozesse. Nicht leichtfertig. Nicht billig. Nicht ohne Berater. Und natürlich hatte er eine Cyberversicherung.

„Haben Sie neu gestartet?“, fragte er.

Er hörte selbst, wie falsch der Satz war. Der erste Reflex eines Menschen, der sein Leben lang Probleme gelöst hat: ausmachen, anmachen, weiter.

„Zweimal“, sagte Keller.

„Dann nichts mehr anfassen. Ich bin in zwanzig Minuten da.“

Er brauchte siebzehn. Die Zufahrt zum Werk war beleuchtet wie immer. Das Schild am Tor sah aus wie immer. Hartmann Maschinenbau GmbH. Präzision seit drei Generationen.

Nur die Gesichter passten nicht zum Morgen.

Auf dem Parkplatz standen schon mehr Autos als üblich. In der Halle brannte das harte weiße Licht, das keine Ausreden zulässt. Einige Mitarbeiter der Frühschicht waren bereits da, Jacken offen, Sicherheitsschuhe an, Hände in den Taschen. Niemand fluchte. Das war das Schlimmste. Fluchen ist manchmal ein gutes Zeichen. Es bedeutet, dass Menschen noch glauben, mit Kraft etwas bewegen zu können.

Der Produktionsleiter kam ihm entgegen. Normalerweise hatte Keller immer etwas in der Hand: einen Plan, ein Tablet, einen Ordner, einen Lieferschein. Heute hatte er nichts in der Hand.

„Zeigen Sie es mir“, sagte Hartmann.

Sie gingen in die Arbeitsvorbereitung. Auf dem Bildschirm stand weißer Text auf dunklem Grund. Keine normale Fehlermeldung. Kein Fenster, das man wegklickt. Keine Störung, die sich mit einem Neustart erledigt.

„Your files have been encrypted.“

Ihre Daten wurden verschlüsselt. Darunter eine Adresse. Eine Frist. Ein Betrag. Sätze in kaltem Englisch, geschrieben nicht für Maschinen, sondern für Menschen. Für den Puls. Für den Magen. Für die Stelle im Körper, an der Verantwortung plötzlich Gewicht bekommt. Hartmann las den Text zweimal. Beim zweiten Mal verstand er nicht mehr. Er verstand weniger.

„Das passiert doch nur den anderen“, sagte er.

Niemand antwortete. Der Satz blieb im Raum stehen. Thomas Hartmann war kein leichtsinniger Mann. Er las Zeitung. Er kannte die Berichte über Krankenhäuser, Stadtverwaltungen, große Konzerne, die tagelang nicht arbeiten konnten. Er hatte darüber in Unternehmerkreisen gesprochen. Mit ernstem Gesicht. Mit dem richtigen Kopfnicken.

„Schlimm“, hatte er gesagt.

„Da muss man wirklich etwas tun.“

Man. Nicht ich. Jetzt stand er vor dem Bildschirm seines eigenen Unternehmens. Herr Baumann, der IT-Leiter, kam wenige Minuten später mit nassen Haaren und einem Rucksack über der Schulter durch die Tür. Er war ein ruhiger Mann. An normalen Tagen schätzte Hartmann diese Ruhe. An diesem Morgen machte sie ihn nervös.

„Ich brauche alle betroffenen Systeme vom Netz“, sagte Baumann.

„Wie lange dauert das?“

„Das weiß ich noch nicht.“

„Dann schätzen Sie.“

Baumann sah ihn an.

„Eine Schätzung wäre im Moment reine Spekulation.“

Hartmann hätte ihn dafür anfahren können. An einem normalen Tag vielleicht. Aber Baumanns Gesicht hielt ihn zurück. Es war nicht panisch. Es war konzentriert.

„Können wir das Backup einspielen?“

„Vielleicht.“

„Vielleicht?“

„Erst müssen wir wissen, was sauber ist.“

Vielleicht. In einem Maschinenbauunternehmen war vielleicht kein Zustand. Ein Teil passte oder passte nicht. Eine Maschine lief oder lief nicht. Ein Liefertermin hielt oder hielt nicht. Vielleicht war etwas für Wetterberichte. Nicht für die Frühschicht. Hartmann griff zum Handy.

„Wen rufen Sie an?“, fragte Keller.

„Den Versicherungsmakler.“

Wieder ein Reflex. Nicht falsch, aber zu früh. Der Makler ging nicht ran. Natürlich nicht. Es war kurz vor sechs. Hartmann starrte auf das Handy, als könne sich darin die Ordnung der Welt wiederherstellen. Dann rief er Frau Weber an, die kaufmännische Leiterin.

„Bitte kommen Sie sofort ins Werk. Ein Cybervorfall. Bringen Sie die Policenmappe mit. Und die Notfallnummern, falls wir welche haben.“

Falls wir welche haben. Er hörte sich selbst zu und mochte den Satz nicht. Im Bürotrakt roch es nach Reinigungsmittel und altem Kaffee. Im Besprechungsraum sammelten sich die Menschen, die sonst Antworten hatten: Produktion, IT, kaufmännische Leitung, Versand, Einkauf, Vertrieb. Jeder brachte ein Stück Wirklichkeit

mit. Und jedes Stück war unangenehm. Die Lieferanten würden ab acht Uhr anrufen. Die Kunden warteten auf Sendungsnummern. Ein Lkw stand bereits an Tor drei. Die Fertigung konnte einzelne Aufträge aus dem Gedächtnis beginnen, aber niemand wollte Ausschuss produzieren, nur damit es nach Bewegung aussah. Die Cloud-Oberfläche war nicht erreichbar. Einige lokale Dateien zeigten dieselbe Lösegeldforderung. Auf einem Bildschirm im Leitstand blinkte noch immer die Nachricht der Angreifer.

Hartmann hörte zu. Er fragte. Er unterbrach. Er wurde lauter. Dann wieder leiser. Sein Kopf versuchte, aus der Lage ein normales Problem zu machen: Zuständigkeit finden, Aufgabe zuweisen, Druck erhöhen, Ergebnis verlangen. So hatte er das Unternehmen geführt. Nicht schlecht. Profitabel. Solide. Angesehen.

Aber an diesem Morgen konnte er niemandem erklären, warum niemand arbeiten konnte.

„Wir haben doch die Versicherung“, sagte Weber, als sie die Mappe auf den Tisch legte.

Es sollte beruhigen. Tat es aber nicht. Die Mappe war ordentlich. Register. Deckblatt. Policennummer. Ansprechpartner. Alles, was Papier tun kann, war getan. Aber Papier fährt keine Produktion hoch. Papier ruft keine Kunden an. Papier entscheidet nicht, ob man zahlt, meldet, schweigt, trennt, wiederherstellt oder erst einmal Ordnung schafft.

Hartmann setzte sich zum ersten Mal an diesem Morgen. Draußen vor der Glaswand standen Mitarbeiter. Nicht neugierig. Wartend. Sie sahen nicht auf Herrn Baumann. Sie sahen nicht auf Herrn Keller. Sie sahen nicht auf Frau Weber. Sie sahen auf ihn. Da begriff Hartmann etwas, das ihm niemand in dieser Deutlichkeit gesagt hatte:

In der Krise schaut ein Unternehmen nicht auf die IT.

Es schaut auf die Spitze.

Und wenn die Spitze nur Nebel sendet, wird unten niemand klarer. Die Geschichte dieses Buches beginnt deshalb nicht mit einer De-

finition, sondern mit einem Anruf. Weil genau dort die Illusion endet, Cyber sei ein technisches Randthema. Cyber ist nicht nur Firewall, Passwort und Serverraum. Cyber berührt die Lebensadern des Unternehmens: Lieferfähigkeit, Liquidität, Reputation, Versicherung, Datenschutz, Haftung, Menschen.

Wenn diese Adern unter Druck geraten, reicht es nicht, wenn irgendwo ein Ticket eröffnet wird. Dann braucht es Führung. Nicht Allwissenheit. Nicht Heldentum. Nicht den Geschäftsführer, der nachts selbst am Server schraubt.

Es braucht Ordnung.

Wer entscheidet?

Wer dokumentiert?

Wer spricht mit Kunden?

Wer meldet an wen?

Wer prüft die Versicherung?

Wer hält die Mitarbeiter ruhig?

Wer stellt sicher, dass nicht aus Panik Beweise gelöscht werden?

Wer weiß, ob die Backups funktionieren?

Wer kann später zeigen, was getan wurde?

Das sind keine Fragen an den Maschinenraum. Das sind Fragen an die Geschäftsleitung. Die Hartmann Maschinenbau GmbH gibt es nicht, sie wurde für dieses Buch erfunden. Aber der Anruf um 05:17 Uhr ist keine Erfindung.

Solche Anrufe gibt es. Mal ruft der Produktionsleiter an, mal der IT-Dienstleister, mal die Tochter, die im Unternehmen arbeitet. Der Satz klingt fast immer gleich:

| „Wir kommen nicht rein.“

Der Fehler entsteht selten um 05:17 Uhr. Um 05:17 Uhr wird er nur sichtbar. Er entsteht Monate vorher. In der Sitzung, in der man sagt: „Das machen wir später.“ Beim Budget, das noch eine Runde warten soll. Beim Backup, das zwar läuft, aber nie getestet wurde.

Bei der Schulung, die als lästig gilt. Bei der KI-Anwendung, die im Vertrieb genutzt wird, ohne dass jemand sie freigegeben hat. Bei der Versicherung, deren Antrag besser aussieht als die Wirklichkeit. Beim Protokoll, in dem steht: „IT kümmert sich.“

Jeder einzelne Punkt wirkt klein. Zusammen können sie ein Unternehmen in die Knie zwingen. Dieses Buch will keine Angst machen. Es will etwas anderes: Es will zeigen, wie Unternehmer wieder handlungsfähig werden, bevor der Bildschirm schwarz wird.

Thomas Hartmann wird in diesem Buch weitergehen. Nicht als Held. Helden sind im echten Unternehmensleben selten und meistens teuer. Er wird Fehler machen, widersprechen, zu spät verstehen und dann doch handeln. So wie Menschen handeln, wenn ein Thema zu groß, zu technisch, zu juristisch oder schlicht zu unbequem erscheint.

Wir rollen die Krise rückwärts auf. Nicht, um klüger zu wirken als der Mann, der an diesem Morgen im Hallenlicht vor stehenden Maschinen steht. Sondern damit Sie früher klug sein können. Um 06:03 Uhr kam die Frühschicht durch die Tür. Die Mitarbeiter erwarteten einen normalen Tag. Material rein, Teile raus, Qualität prüfen, ausliefern.

Stattdessen standen sie in einer hellen Halle, in der Maschinen schwiegen und Bildschirme Befehle von Fremden zeigten. Hartmann trat aus dem Besprechungsraum. Er hatte noch keine Lösung. Aber er hatte begriffen, dass sein erster Job nicht darin bestand, so zu tun, als gäbe es eine. Sein erster Job war Ordnung. Ruhe. Richtung.

Er sah Keller an, dann Baumann, dann Weber.

„Wir machen jetzt keine Show“, sagte er. „Wir machen Führung.“

Das war noch nicht genug. Aber es war der erste richtige Satz des Tages. Und bevor wir klären, was in den nächsten Stunden, Tagen

und Wochen zu tun ist, müssen wir eine Frage aus dem Weg räumen, die in vielen Unternehmen vorher gestellt wird. Meistens mit einem kleinen Lächeln. Manchmal mit echter Überzeugung.

| „Wir sind doch kein Krankenhaus.“

Genau dort beginnt die Reise.

Die Krise begann früher

Wir halten diesen Morgen jetzt an.

Nicht, weil die Krise vorbei wäre. Sondern weil sie nicht an diesem Morgen begonnen hat.

Der Angriff wurde um 05:17 Uhr sichtbar. Entstanden ist die Verwundbarkeit Monate vorher – in Annahmen, Protokollen, Budgets, Zuständigkeiten, Versicherungsanträgen, ungetesteten Backups, unregelmäßiger KI-Nutzung und unbequemen Fragen, die niemand stellte.

Deshalb kommt jetzt die Rückblende. Sie schaut nicht auf Technik. Sie schaut auf Führung.

Die erste Spur der Rückwärtssuche führt zurück zu einem Satz, der an einem ganz normalen Dienstag fiel:

| „Wir sind doch kein Krankenhaus.“

4 | **Wir sind doch kein Krankenhaus**

Der Satz fiel nicht in einer Krise. Das ist wichtig. Er fiel an einem normalen Dienstag, kurz nach halb zwölf, in einem Besprechungsraum mit zu großem Tisch und zu kleinem Fenster. Auf dem Tisch standen Mineralwasser, zwei Tassen Kaffee und ein Teller mit Keksen, von denen niemand einen nahm. Draußen lief die Fertigung. Man hörte durch die Wand das entfernte Pochen einer Maschine, die seit Jahren tat, was man von ihr verlangte. Mit am Tisch saß ein externer Sicherheitsberater, den Frau Weber eingeladen hatte – der Einzige an diesem Vormittag, der nicht zum Haus gehörte.

Thomas Hartmann lehnte sich zurück, faltete die Hände über dem Bauch und sagte mit der ruhigen Freundlichkeit eines Mannes, der die Sache für erledigt hielt, bevor sie angefangen hatte:

„Mit allem Respekt – wir sind doch kein Krankenhaus.“

IT-Leiter Baumann sah plötzlich sehr interessiert in seinen Kaffeebecher. Weber, die kaufmännische Leiterin, machte sich eine Notiz. Vielleicht nur ein Wort. Vielleicht den Satz, der im Raum stand.

Hartmann lächelte. Nicht spöttisch. Nicht arrogant. Eher so, wie Unternehmer lächeln, wenn sie glauben, eine Diskussion auf den Boden der Tatsachen zurückzuholen. Krankenhäuser, Stadtverwaltungen, Energieversorger, große Konzerne – ja. Da konnte man sich Cyberangriffe vorstellen. Aber ein mittelständischer Maschinenbauer mit hundertachtzig Mitarbeitern? Eine Firma, die seit drei Generationen zuverlässig Teile produziert, Kunden beliefert, Löhne zahlt, Investitionen plant?

„Wir sind doch kein Krankenhaus.“

Der Berater nickte. Er kennt diesen Satz und das Nicken, das er auslöst – nicht, weil der Satz richtig ist, sondern weil er verständlich ist. Er klingt nach gesundem Menschenverstand. Nach Bodenhaftung. Nach Unternehmensführung, die sich nicht von jeder Schlagzeile treiben lässt. In Wahrheit steckt darin aber eine gefährliche

Annahme: Wir sind nicht wichtig genug. Genau hier beginnt das Problem.

Der Irrtum, der vernünftig klingt

Die meisten gefährlichen Sätze im Unternehmen klingen zunächst vernünftig.

„Das haben wir immer so gemacht.“

„Das machen wir später.“

„Dafür ist die IT zuständig.“

„Uns trifft das nicht.“

„Wir sind doch kein Krankenhaus.“

Keiner dieser Sätze ist böse gemeint. Oft entstehen sie aus Erfahrung. Aus Pragmatismus. Aus dem Wunsch, nicht jedem neuen Risiko hinterherzulaufen. Unternehmer müssen täglich entscheiden, was wichtig ist und was warten kann. Wer jedes Thema zur Chefsache macht, führt am Ende gar nichts mehr.

Aber Cyber ist kein normales Zusatzthema mehr.

Cyber betrifft nicht nur Computer. Cyber betrifft Abhängigkeiten. Und Abhängigkeiten hat heute jedes Unternehmen, das digital arbeitet, vernetzt produziert, Daten verarbeitet, Lieferketten bedient, Kundenportale nutzt, Rechnungen stellt, Mitarbeiter beschäftigt oder KI-Werkzeuge einsetzt.

Hartmann dachte, sein Unternehmen sei zu unauffällig. In Wahrheit war es abhängig. Das ist der entscheidende Unterschied.

Ein Angreifer fragt nicht zuerst, ob Ihr Unternehmen berühmt ist. Er fragt nicht, ob Ihr Name in der Zeitung steht oder ob Sie kritische Infrastruktur betreiben. Sehr oft fragt er gar nichts. Automatisierte Systeme suchen nach offenen Zugängen, alten Passwörtern, ungepatchten Systemen, erreichbaren Fernwartungen, schlecht geschützten Backups oder Menschen unter Zeitdruck.

Sie werden nicht immer ausgewählt. Sie werden oft gefunden. Das klingt nüchtern. Genau deshalb ist es wichtig.

Der moderne Angriff ist nicht immer der gezielte Schlag gegen den ganz großen Namen. Häufig ist er ein Geschäft mit Masse, Geschwindigkeit und Gelegenheit. Wer erreichbar ist, kann getroffen werden. Wer abhängig ist, kann erpresst werden. Wer Teil einer Lieferkette ist, kann als Einstiegspunkt interessant werden.

Die Hartmann Maschinenbau GmbH war kein Krankenhaus. Aber sie hatte eine Produktion, die ohne digitale Systeme nicht sauber laufen konnte. Sie hatte Konstruktionsdaten, die über Jahrzehnte entstanden waren. Sie hatte ein Cloud-ERP, in dem Aufträge, Liefertermine, Preise, Kundendaten und Zahlungsinformationen zusammenliefen.

Die Firma hatte Fernwartungszugänge für Maschinen. Sie hatte Mitarbeiter, die täglich E-Mails, Anhänge, Zahlungsanweisungen und Kundenkommunikation bearbeiteten. Sie hatte große Kunden, für die ihre Lieferfähigkeit wichtig war. Und sie hatte begonnen, KI im Vertrieb zu nutzen, ohne dass jemand den Überblick darüber behielt, wer damit was machte. Das ist mehr als genug. Nicht, weil das Unternehmen besonders schlecht aufgestellt war. Im Gegenteil. Es war modern. Und genau darin lag ein Teil des Risikos.

Digitalisierung: Leistung und Abhängigkeit

Viele Unternehmer haben Digitalisierung als Fortschritt erlebt. Zu Recht. Das ERP machte Abläufe schneller. Die Fertigung wurde transparenter. Der Versand konnte sauberer planen. Kunden erhielten verlässlichere Informationen. Die Buchhaltung arbeitete effizienter. Der Vertrieb konnte Angebote international schneller vorbereiten. Daten standen dort zur Verfügung, wo Entscheidungen getroffen wurden.

Digitalisierung hat aus vielen Unternehmen bessere Unternehmen gemacht.

Aber sie hat auch etwas verändert, das nicht immer offen ausgesprochen wird: Sie hat die Abhängigkeit von funktionierenden Systemen massiv erhöht.

Früher konnte ein Unternehmen bei einer Störung vielleicht noch ein paar Tage improvisieren. Ordner, Fax, Telefon, Zuruf, Erfahrungswissen. Nicht schön, aber möglich. Heute steckt der Betrieb oft so tief in digitalen Prozessen, dass ein Ausfall nicht nur unbequem ist, sondern existenziell werden kann.

Ohne ERP keine Auftragsklarheit.

Ohne Produktionsdaten keine saubere Fertigung.

Ohne Kundendaten keine Kommunikation.

Ohne E-Mail keine Abstimmung.

Ohne funktionierende Zugänge kein Versand.

Ohne geprüfte Backups keine schnelle Wiederherstellung.

Das ist keine Kritik an Digitalisierung. Es ist ihre zweite Seite.

Wer digital leistungsfähiger wird, muss digital widerstandsfähiger werden.

Hartmann hatte den ersten Teil verstanden. Den zweiten noch nicht ausreichend.

Er hatte investiert, modernisiert, optimiert. Aber er hatte Cybersicherheit noch immer als Begleitthema verstanden. Als etwas, das Baumann im Hintergrund bearbeitet. Als technische Voraussetzung, nicht als Führungsfrage.

Diese Trennung funktioniert heute nicht mehr.

Die Frage ist nicht: Haben wir IT?

Die Frage ist: Können wir weiterführen, wenn die IT ausfällt?

„Schön und gut“, sagte Hartmann, der dem Berater zugehört hatte. „Aber warum wir? Was sollen die denn bei uns holen? Wir machen Maschinen. Wir haben keine Patientenakten.“

Die Frage ist berechtigt.

Sie wird nur oft zu eng gestellt.

Viele Unternehmer denken bei Cyberangriffen zuerst an Datenklau. An personenbezogene Daten, Gesundheitsakten, Kreditkartennummern, Passkopien. Natürlich sind solche Daten sensibel. Aber ein Angriff muss nicht immer deshalb wirken, weil Daten besonders spektakulär sind.

Er wirkt, wenn der Ausfall teuer ist.

Bei einem Maschinenbauer können Angreifer sehr viel treffen:

Die Produktion.

Wenn die Produktion steht, entstehen Kosten, Lieferverzug, Vertragsdruck und Kundenunruhe.

Die Konstruktionsdaten.

Zeichnungen, Spezifikationen, technische Dokumentationen und Entwicklungswissen sind nicht nur Dateien. Sie sind Unternehmenssubstanz.

Das ERP.

Dort liegen Aufträge, Preise, Kunden, Lieferanten, Zahlungsdaten, Termine, Lagerbestände und Kalkulationen.

Die Lieferkette.

Ein Mittelständler ist oft Teil größerer industrieller Abläufe. Wenn er ausfällt, spürt es nicht nur er selbst.

Das Vertrauen.

Kunden fragen sich nach einem Vorfall nicht nur, ob ein Unternehmen Opfer wurde. Sie fragen, ob es vorbereitet war.

Die Versicherung.

Im Schadensfall interessiert den Versicherer nicht nur, dass eine Police existiert. Er fragt, welche Maßnahmen zugesichert und tatsächlich umgesetzt waren.

Die Geschäftsleitung.

Wenn später geprüft wird, was organisiert, entschieden, überwacht und dokumentiert wurde, ist Cyber nicht mehr nur ein technischer Vorfall. Es ist ein Führungsvorgang.

Hartmann hörte zu. Sein Lächeln war schmaler geworden.

„Sie meinen, es geht nicht nur darum, ob jemand unsere Daten will.“

„Genau“, sagte der Berater. „Es geht darum, ob jemand Ihr Unternehmen unter Druck setzen kann.“

Das ist der Kern.

Ein Erpresser muss nicht lieben, was Sie haben. Es reicht, wenn er weiß, dass Sie es dringend brauchen.

Der Kunde fragt früher als die Behörde

Während des Gesprächs, vibrierte Hartmanns Handy.

Er sah auf das Display und runzelte die Stirn.

„Entschuldigung.“

Er öffnete eine E-Mail. Der Absender war einer seiner großen Kunden. Ein Industriekonzern, dessen Name auf großen Werbetafeln, Messen und Geschäftsberichten auftauchte. Betreff:

„Lieferantenbewertung Informationssicherheit – Selbstauskunft“

Hartmann las. Dann legte er das Handy auf den Tisch.

„Das passt ja jetzt gut.“

Weber sah ihn an.

„Was ist es?“, fragte sie.

„Ein Fragebogen. Informationssicherheit. Lieferkette. Mehr-Faktor-Anmeldung. Notfallkonzept. Wiederherstellungstest. Dienstleisterzugänge.“

Baumann griff zum Wasserglas.

Das ist der Moment, in dem viele Unternehmer zum ersten Mal verstehen, dass Cyber nicht nur über Behörden in ihr Unternehmen kommt. Manchmal kommt es über den Kunden.

Nicht als Bußgeldbescheid.

Sondern als Fragebogen.

Nicht mit Frist aus dem Gesetzblatt.

Sondern mit Frist aus dem Einkauf.

Und der letzte Satz solcher Schreiben klingt selten dramatisch. Er ist oft höflich formuliert. Aber seine wirtschaftliche Bedeutung ist klar:

„Eine fehlende oder unzureichende Rückmeldung kann Auswirkungen auf die Lieferantenbewertung haben.“

Das heißt in Unternehmerdeutsch:

„Wir können auch andere fragen.“

Hartmann las den Anhang. Die Fragen waren nicht böse. Sie waren sachlich. Gerade das machte sie unangenehm.

Haben Sie ein Informationssicherheitskonzept?

Werden externe Zugänge mit Mehr-Faktor-Authentifizierung geschützt?

Wann wurde der letzte Wiederherstellungstest durchgeführt?

Wie werden Dienstleister mit Zugriff auf produktionsnahe Systeme geprüft?

Gibt es einen dokumentierten Notfallplan?

Gibt es Schulungen der Mitarbeiter?

Der Geschäftsführer blickte zu seinem IT-Leiter.

Herr Baumann sagte nichts.

Frau Weber machte wieder eine Notiz. Diesmal schrieb sie länger.

„Das ist doch nicht von einer Behörde“, sagte Hartmann.

„Nein“, sagte der Berater. „Das ist von Ihrem Umsatz.“

Der Satz blieb einen Moment stehen.

Genau hier ändert sich die Perspektive. Viele Unternehmer fragen: Sind wir gesetzlich betroffen? Das ist wichtig. Aber es ist nur eine Frage. Die zweite lautet: Was verlangen unsere Kunden, Banken, Versicherer und Geschäftspartner?

Selbst wenn ein Unternehmen rechtlich nicht in allen Punkten unmittelbar betroffen wäre, kann es wirtschaftlich sehr schnell in die Pflicht geraten. Große Unternehmen geben Anforderungen in die Lieferkette weiter. Versicherer fragen beim Antrag nach Sicherheitsmaßnahmen. Banken interessieren sich für operationelle Risiken. Kunden verlangen Nachweise.

Cybersicherheit wird damit zum Teil der Marktteilnahme.

Vor zwanzig Jahren war Qualitätsmanagement für viele Mittelständler ein Reizwort. Heute fragt niemand mehr grundsätzlich, ob Qualität dokumentiert werden muss. Sie ist Eintrittskarte.

Cybersicherheit geht denselben Weg.

Erst wird gestöhnt.

Dann wird geprüft.

Dann wird ausgewählt.

Der gefährliche Trost der Versicherung

„Wir haben ja eine Cyber-Police“, sagte Weber.

Sie sagte es nicht leichtfertig. Sie sagte es wie die kaufmännische Leiterin, die ihre Hausaufgaben gemacht hatte. Das hatte sie. Die Police existierte. Der Vertrag war ordentlich abgelegt. Die Prämie bezahlt.

Das ist gut.

Aber es reicht nicht.

Eine Versicherung ist kein Ersatz für Organisation. Sie ist ein Baustein im Umgang mit Restrisiko. Im Schadensfall fragt der Versicherer nicht nur, ob ein Angriff stattgefunden hat. Er prüft auch,

welche Angaben beim Abschluss gemacht wurden, welche Sicherheitsmaßnahmen vereinbart waren, welche Obliegenheiten bestanden und ob das Unternehmen im Vorfeld und im Schadensfall richtig gehandelt hat.

Viele Unternehmer glauben: Wenn es digital ist, ist es Cyber. Und wenn es Cyber ist, zahlt die Cyberversicherung.

So einfach ist es nicht.

Eine Police kann Forensik, Wiederherstellung, Betriebsunterbrechung, Krisenkommunikation oder bestimmte Drittschäden abdecken. Aber der konkrete Umfang steht im Vertrag. Und der Vertrag baut auf Voraussetzungen.

Wenn im Antrag steht, dass externe Zugänge mit Mehr-Faktor-Authentifizierung geschützt sind, sollte das in der Wirklichkeit auch stimmen.

Wenn regelmäßige Backups zugesichert werden, sollte nicht nur die Sicherung laufen, sondern die Wiederherstellung getestet sein.

Wenn Schulungen angegeben werden, sollten sie nicht nur geplant, sondern dokumentiert sein.

Wenn ein Notfallplan existiert, sollte er im Ernstfall erreichbar sein – nicht nur als Datei in einem System, das gerade verschlüsselt wurde.

Hartmann hörte aufmerksam zu.

„Sie sagen also, die Versicherung schützt uns nicht vor der Frage, ob wir ordentlich gearbeitet haben.“

„Genau.“

Das ist keine schlechte Nachricht. Es ist eine nützliche.

Denn vieles, was der Versicherer fragt, ist auch das, was eine vernünftige Geschäftsleitung ohnehin wissen sollte. Die Police ist damit nicht nur Schutzinstrument. Sie ist auch ein Spiegel. Sie zeigt, welche Mindestannahmen über Ihre Sicherheitsorganisation bestehen.

Man sollte diesen Spiegel nicht erst betrachten, wenn der Schaden eingetreten ist.

Der Mensch ist kein Randthema

Bis zu diesem Zeitpunkt hatte das Gespräch vor allem Systeme, Kunden, Versicherungen und Lieferketten behandelt. Dann kam Weber auf einen Punkt zurück, der in vielen Unternehmen zu spät behandelt wird.

„Was ist mit den Mitarbeitern?“, fragte die kaufmännische Leiterin.

„Das ist wahrscheinlich der wichtigste Punkt“, sagte der eingeladene Berater.

Viele Angriffe beginnen nicht mit einem genialen technischen Einbruch. Sie beginnen mit einem normalen Arbeitstag. Einer E-Mail. Einer neuen Bankverbindung. Einem Link. Einer angeblichen Rechnung. Einer Nachricht, die dringend klingt und vertraulich sein soll.

Der Mensch wird dann nicht angegriffen, weil er dumm ist.

Er wird angegriffen, weil er arbeitet.

Weil er helfen will.

Weil er den Chef nicht enttäuschen möchte.

Weil er eine Frist sieht.

Weil er unter Druck steht.

Weil eine Nachricht heute so gut formuliert sein kann, dass man sie nicht mehr an Rechtschreibfehlern erkennt.

Künstliche Intelligenz verschärft diese Lage. Phishing-Mails werden sprachlich besser. Betrugsversuche können persönlicher wirken. Stimmen lassen sich imitieren. Texte können den im Unternehmen üblichen Tonfall nachahmen. Was früher auffiel, klingt heute professionell.

Das bedeutet nicht, dass jeder Mitarbeiter zum Sicherheitsexperten werden muss.

Aber es bedeutet, dass Unternehmen klare Regeln brauchen:

Wann wird zurückgerufen?

Welche Zahlungen brauchen eine zweite Freigabe?

Wie werden neue Bankverbindungen geprüft?

Was ist bei ungewöhnlicher Dringlichkeit zu tun?

Wo meldet man Verdachtsfälle?

Wird ein Mitarbeiter gelobt oder kritisiert, wenn er lieber einmal zu viel fragt?

Gerade der letzte Punkt ist entscheidend.

Eine Sicherheitskultur entsteht nicht durch Folien. Sie entsteht durch Verhalten. Wenn Mitarbeiter Angst haben, einen Verdacht zu melden, weil sie nicht als störend gelten wollen, ist das Unternehmen verwundbar. Wenn sie wissen, dass Nachfragen erwünscht ist, entsteht ein Schutz, den keine Software allein leisten kann.

Hartmann sagte lange nichts.

Dann fragte er:

| „Haben wir so eine Rückrufregel eigentlich?“

Weber sah zu Baumann.

Baumann sah auf den Tisch.

Damit war die Antwort gegeben.

KI: Das neue Werkzeug ohne Inventarliste

Gegen Ende des Gesprächs erwähnte Baumann einen weiteren Punkt.

| „Wenn wir ohnehin darüber sprechen: Im Vertrieb nutzen einige Kollegen ein KI-Werkzeug für Angebotsmails.“

Hartmann drehte sich zu ihm.

| „Welche Kollegen?“

„Das müsste ich prüfen.“

„Welche Daten gehen da rein?“

Baumann schwieg.

Hartmann sah zu Weber.

„Wissen Sie davon?“

„Nein.“

Das ist ein typischer Moment in Unternehmen im Jahr 2026.

KI ist nicht irgendwann. KI ist schon da.

Nicht immer als großes strategisches Projekt. Oft als kleines Werkzeug im Alltag. Jemand lässt eine E-Mail formulieren. Jemand übersetzt einen Kundentext. Jemand fasst ein Protokoll zusammen. Jemand lädt eine Tabelle hoch, um schneller eine Auswertung zu bekommen. Jemand baut einen Chatbot auf die Website, weil es modern wirkt.

Jeder einzelne Vorgang erscheint harmlos.

Zusammen entsteht ein ungeregelter Raum.

Die Frage ist nicht, ob Unternehmen KI nutzen sollten. Sie werden es tun. Viele tun es bereits. Die Frage ist, ob die Geschäftsleitung weiß, wo KI eingesetzt wird, mit welchen Daten, zu welchem Zweck und mit welcher Kontrolle.

Denn KI kann nützlich sein. Sehr nützlich sogar.

Aber sie kann auch falsche Sicherheit erzeugen. Sie formuliert überzeugend, auch wenn der Inhalt falsch ist. Sie verarbeitet möglicherweise Daten, die dort nicht hingehören. Sie erzeugt Texte, die im Namen des Unternehmens nach außen gehen. Sie kann Kundenerwartungen, Haftung, Datenschutz und Geschäftsgeheimnisse berühren.

Ein Unternehmer muss dafür kein KI-Forscher werden.

Aber er braucht eine KI-Inventur.

Welche Werkzeuge werden genutzt?

Von wem?

Mit welchen Daten?

Für welche Zwecke?

Wer prüft die Ergebnisse?

Was darf nie eingegeben werden?

Was darf nie ungeprüft nach außen gehen?

Das ist keine Innovationsbremse. Es ist die Voraussetzung dafür, dass Innovation nicht zum Blindflug wird.

Hartmann lehnte sich zurück.

„Ich dachte, heute sprechen wir über Cyber.“

„Tun wir“, sagte der Berater.

„Aber jetzt sind wir bei KI.“

„Genau deshalb gehört das Thema auf Ihren Tisch.“

Cyber, Datenschutz und KI sind im Unternehmen keine getrennten Welten mehr. Sie treffen dieselben Prozesse, dieselben Menschen und oft dieselben Daten. Wer sie getrennt betrachtet, übersieht die Verbindungen.

Der Mitarbeiter, der eine Phishing-Mail erhält, nutzt vielleicht gleichzeitig ein KI-Tool.

Der Vertrieb, der Kundendaten verarbeitet, formuliert vielleicht KI-gestützte Angebote.

Der Dienstleister, der eine Website betreut, bindet vielleicht einen Chatbot ein.

Der Versicherer fragt nach Sicherheitsmaßnahmen, die auch KI-Prozesse betreffen können.

Der Kunde will nicht wissen, ob Ihr Problem aus IT, Datenschutz oder KI stammt. Er muss wissen, ob er Ihnen weiter vertrauen kann.

Eine lästige Pflicht wird zum Verkaufsargument

In diesem Moment schob Hartmann den Kundenfragebogen wieder vor sich.

„Also gut“, sagte er. „Nehmen wir an, wir müssen das ernst nehmen. Dann ist das doch vor allem Aufwand.“

„Ja“, erwiderte der Berater. „Aber nicht nur.“

Cybersicherheit wird häufig als Last beschrieben. Mehr Pflichten. Mehr Dokumentation. Mehr Kosten. Mehr Schulungen. Mehr Prüfungen.

Das stimmt teilweise. Aber es ist nur die halbe Wahrheit.

Die andere Hälfte lautet: Wer Sicherheit nachweisen kann, wird verlässlicher.

Für Kunden.

Für Banken.

Für Versicherer.

Für Beiräte.

Für Käufer.

Für Nachfolger.

Ein Unternehmen, das seine Risiken kennt, seine Maßnahmen dokumentiert, seine Mitarbeiter schult, seine Dienstleister prüft, seine KI-Nutzung ordnet und seinen Notfallplan getestet hat, sendet ein Signal:

Wir sind nicht unverwundbar. Aber wir führen.

Das ist ein Unterschied.

Kein Kunde erwartet absolute Sicherheit. Wer diese verspricht, macht sich unglaubwürdig. Aber Kunden erwarten, dass ein Unternehmen seine Hausaufgaben gemacht hat. Gerade in Lieferketten wird das zunehmend wichtig. Wer hier vorbereitet ist, beantwortet Fragebögen schneller, verhandelt besser und steht im Vergleich zu weniger geordneten Wettbewerbern stärker da.

Hartmann sah auf den Fragebogen.

„Sie meinen, das kann auch ein Vorteil sein?“

„Ja. Wenn Sie es nicht nur machen, um einen Haken zu setzen.“

Das ist entscheidend.

Wer Cybersicherheit nur als Pflichtübung versteht, wird Formulare produzieren. Wer sie als Führungsaufgabe versteht, baut Substanz.

Substanz heißt nicht, dass nichts passieren kann.

Substanz heißt, dass ein Unternehmen im Ernstfall nicht planlos wird.

Die erste ehrliche Bestandsaufnahme

Am Ende dieses Dienstags war bei Hartmann Maschinenbau nichts gelöst.

Aber etwas hatte sich verändert.

Der Satz „Wir sind doch kein Krankenhaus“ hatte seine beruhigende Wirkung verloren.

Nicht, weil Hartmann plötzlich glaubte, sein Unternehmen sei ein Krankenhaus. Sondern weil er verstand, dass der Vergleich falsch war. Entscheidend war nicht nur die Branche. Es ging auch um Abhängigkeit, Erreichbarkeit, Daten, Lieferketten, Menschen und Verantwortung.

Weber nahm ein neues Blatt.

„Dann machen wir eine Liste“, sagte sie.

Hartmann nickte.

„Welche?“

„Eine ehrliche.“

Das war ein guter Anfang.

Die Liste hatte fünf Überschriften:

1. Wovon hängt unser Betrieb digital ab?

2. Welche Kunden verlangen heute schon Nachweise?
3. Welche Dienstleister haben Zugriff auf unsere Systeme?
4. Welche Sicherheitsmaßnahmen behaupten wir – und welche können wir belegen?
5. Wo wird im Unternehmen KI genutzt?

Baumann ergänzte:

„Und welche Zugänge sind alt.“

Hartmann sah ihn an.

„Gibt es da etwas, das ich wissen sollte?“

Baumann zögerte.

Dieses Zögern war Antwort genug.

„Es gibt einen Fernwartungszugang für Linie drei. Alt. Selten genutzt. Ich muss prüfen, wie er abgesichert ist.“

Hartmann atmete aus.

„Dann fangen wir dort an.“

Es war kein großer Moment. Keine Strategiepräsentation. Kein Projektname. Keine neue Software.

Nur ein Unternehmer, der zum ersten Mal anders an die Sache heranging. Seine Frage lautete jetzt nicht mehr, ob das Unternehmen wichtig genug oder auffällig genug war, um angegriffen zu werden.

Seine Frage lautete jetzt, ob er aufmerksam genug war, um für einen Angreifer keine leichte Beute zu sein.

Memo für die Geschäftsleitung

Nach diesem Kapitel sollten Sie nicht denken: „Wir sind bestimmt betroffen.“

Sie sollten auch nicht denken: „Wir sind bestimmt nicht betroffen.“

Beides wäre zu einfach.

Die richtige Frage lautet:

Was macht unser Unternehmen angreifbar, abhängig oder prüfpflichtig?

Dazu gehören nicht nur Gesetzestexte. Dazu gehören Geschäftsmodell, Kundenstruktur, digitale Abhängigkeiten, Lieferkette, Versicherungsbedingungen, Daten, KI-Nutzung und die Frage, ob Ihre Organisation im Ernstfall handlungsfähig bleibt.

Für die Geschäftsleitung ergeben sich daraus sechs konkrete Fragen:

MEMO

1. Welche digitalen Systeme sind für unsere Lieferfähigkeit unverzichtbar?
2. Welche Daten wären für uns, unsere Kunden oder unsere Mitarbeiter kritisch, wenn sie verschlüsselt, gestohlen oder veröffentlicht würden?
3. Welche Kunden, Banken, Versicherer oder Vertragspartner verlangen heute schon Nachweise zur Informationssicherheit?
4. Welche externen Dienstleister haben Zugriff auf unsere Systeme, Daten oder produktionsnahen Abläufe?
5. Welche KI-Werkzeuge werden im Unternehmen genutzt, offiziell oder inoffiziell?
6. Welche Aussagen über unsere Sicherheit können wir belegen – und welche glauben wir nur?

Diese Fragen sind kein vollständiges Sicherheitskonzept.

Aber sie sind der Anfang von Führung.

Und Führung beginnt selten mit der perfekten Antwort.

Sie beginnt mit der richtigen Frage.

Thomas Hartmann hatte an diesem Dienstag eine solche Frage gefunden.

Nicht mehr:

| „Warum sollten die uns angreifen?“

Sondern:

| „Was würde passieren, wenn sie es tun?“

Damit war der erste Irrtum aus dem Weg.

Der zweite wartete bereits.

Denn wenn ein Unternehmer verstanden hat, dass sein Unternehmen betroffen sein kann, kommt fast automatisch der nächste Satz:

| „Dann soll sich die IT darum kümmern.“

Genau dort beginnt Kapitel 5.

5 | **Das macht doch unsere IT**

Der zweite Satz kam nicht laut. Er kam sogar freundlich.

Thomas Hartmann hatte nach dem Gespräch über den Kundenfragebogen die erste innere Hürde genommen. Er wusste jetzt: Sein Unternehmen war nicht deshalb sicher, weil es kein Krankenhaus war. Es ging auch nicht mehr darum, ob Cyber grundsätzlich wichtig sein konnte. Die Frage war, wer sich darum kümmern sollte.

Sein IT-Leiter Baumann saß ihm gegenüber. Elf Jahre im Haus. Ruhig, zuverlässig, technisch stark. Einer, der Probleme löste, ohne großes Aufsehen zu machen. Einer, dem man vertraute, weil er nie mehr versprach, als er halten konnte.

„Herr Hartmann“, sagte Baumann, „ich kümmere mich darum. Sie müssen sich da nicht einarbeiten.“

Hartmann nickte fast automatisch.

Das war der gefährliche Moment.

Nicht, weil Baumann falsch lag. Natürlich musste die IT eine zentrale Rolle spielen. Kein Geschäftsführer sollte nachts selbst Firewall-Regeln prüfen, Server härten oder Backup-Skripte schreiben. Das wäre nicht Führung, sondern Selbstüberschätzung mit Tastatur.

Gefährlich war etwas anderes: Hartmann wollte die Sache mit diesem Nicken aus seinem Kopf schieben. Er hörte „ich kümmere mich“ und übersetzte innerlich: erledigt.

Genau das funktioniert nicht mehr.

Aufgabe und Verantwortung sind nicht dasselbe

In einem Unternehmen muss delegiert werden. Wer nicht delegiert, führt nicht. Der Meister verantwortet die Maschine, die Buchhaltung die offenen Posten, der Vertrieb den Kundenkontakt, die IT die Systeme. Ohne diese Verteilung wird aus Führung Mikromanagement.

Aber es gibt eine Grenze.

Man kann Aufgaben delegieren. Man kann Verantwortung nicht einfach mit übergeben.

Die IT kann Risiken aufbereiten. Sie kann Maßnahmen vorschlagen. Sie kann Dienstleister steuern, Systeme schützen, Backups einrichten, Logs auswerten, Schulungen vorbereiten und Vorfälle technisch behandeln.

Die Geschäftsleitung muss entscheiden, welche Risiken das Unternehmen trägt, welche Maßnahmen finanziert werden, welche Priorität Cyber im Verhältnis zu Produktion, Vertrieb, Investitionen und Personal bekommt. Sie muss überwachen, ob die beschlossenen Maßnahmen umgesetzt werden. Und sie muss später belegen können, dass sie nicht nur vertraut, sondern geführt hat.

Das ist der Unterschied.

„Baumann macht das“ klingt im Alltag praktisch. Im Ernstfall klingt es dünn.

Denn wenn ein Vorfall passiert, wird später nicht nur gefragt, ob ein Server sicher war. Es wird gefragt: Was hat die Geschäftsleitung gewusst? Was hat sie beschlossen? Was hat sie kontrolliert? Welche Berichte lagen vor? Welche Lücken waren bekannt? Warum wurden sie akzeptiert? Wer hat das entschieden?

Diese Fragen kann Baumann technisch vorbereiten. Beantworten muss sie am Ende Hartmann.

Warum die IT allein nicht entscheiden kann

Hartmann hatte zunächst Mühe mit diesem Gedanken.

„Aber Herr Baumann ist doch der Fachmann“, sagte er.

„Ja“, sagte Frau Weber. „Aber er entscheidet nicht über unser Budget.“

Das war der Satz, der die Diskussion drehte.

Viele Sicherheitsfragen sind in Wahrheit Geschäftsentscheidungen. Nehmen wir ein einfaches Beispiel: Eine alte Maschine in der

Fertigung hat einen Fernwartungszugang. Der Dienstleister kann aus der Ferne helfen, wenn am Wochenende etwas ausfällt. Das ist praktisch. Vielleicht sogar notwendig. Aber der Zugang ist alt, schlecht dokumentiert und nicht mit Mehr-Faktor-Authentifizierung geschützt.

Technisch ist die Antwort klar: absichern, begrenzen, protokollieren, im Zweifel schließen.

Unternehmerisch ist die Antwort schwieriger: Was passiert, wenn die Maschine am Wochenende steht? Was kostet der Stillstand? Wer trägt die Verantwortung für die Freigabe? Welche Alternative gibt es? Welcher Dienstleister wird gebraucht? Wie schnell kann umgestellt werden?

Das kann die IT nicht allein entscheiden.

Oder nehmen wir Backups. Die IT kann sagen, wie oft gesichert wird. Die Geschäftsleitung muss sagen, wie viel Datenverlust das Unternehmen aushält. Eine Stunde? Einen Tag? Eine Woche? Für die Produktion kann die Antwort anders sein als für das Marketingarchiv. Das ist keine technische, sondern eine wirtschaftliche Risikofrage.

Oder Schulungen. Die IT kann Programme, Themen oder Inhalte empfehlen. Die Geschäftsleitung muss klarstellen, dass Teilnahme Pflicht ist, dass Führungskräfte mitmachen, dass Rückfragen erwünscht sind und dass Sicherheitsregeln nicht zum Abhaken in der Agenda gelten, sondern für den alltäglichen Schutz im Betrieb.

Cybersicherheit wird oft zu tief aufgehängt. Sie beginnt im Serverraum und bleibt dort stecken. Dann kann sie technisch sauber aussehen und trotzdem organisatorisch scheitern.

Der Protokollsatz, der später wehtut

Weber öffnete das Protokoll der letzten Geschäftsleitungsrunde. Ein kurzer Punkt stand dort, fast beiläufig:

„IT-Leitung übernimmt NIS-2-/Cyber-Thema“, las sie vor.

Es war kein böser Satz. Er war ordentlich. Er klang nach Zuständigkeit.

Aber genau solche Sätze können später gefährlich werden.

Nicht, weil sie beweisen, dass nichts getan wurde. Sondern weil sie zeigen können, wie ein Thema verstanden wurde. Als IT-Thema. Als operative Aufgabe. Als etwas, das nach unten gegeben wurde.

Hartmann las den Satz noch einmal.

„Was wäre besser?“, fragte er dann.

„Geschäftsleitung behandelt Cyber-Risiken regelmäßig. IT bereitet Lagebild und Maßnahmen vor. Geschäftsleitung entscheidet und überwacht Umsetzung“, urteilte Weber.

Das klang weniger bequem. Aber es war richtiger.

Dokumentation ist nicht nur Verwaltung. Sie zeigt, wie ein Unternehmen denkt. Ein Protokoll kann später entlasten. Es kann aber auch zeigen, dass Verantwortung falsch verstanden wurde.

Deshalb sollte kein Geschäftsleiter den Satz „das macht die IT“ leichtfertig in einem Protokoll stehen lassen.

Die Rolle des Geschäftsführers

Hartmann wollte wissen, was konkret von ihm erwartet wurde.

„Soll ich jetzt jede technische Maßnahme verstehen?“

Nein.

Die Geschäftsführung muss nicht jedes technische Detail verstehen. Sie muss aber genug verstehen, um gute Fragen zu stellen.

Sie muss nicht wissen, wie ein SIEM-System im Detail funktioniert. Aber sie muss wissen, ob sicherheitsrelevante Ereignisse erkannt und bewertet werden.

Sie muss nicht selbst Backups konfigurieren. Aber sie muss wissen, ob die Backups in der Praxis bewiesen haben, dass sie für eine Wiederherstellung taugen und wann das zuletzt erfolgreich getestet wurde.

Die Geschäftsleitung muss nicht jede Schwachstelle kennen. Aber sie muss wissen, ob es ein Verfahren gibt, kritische Schwachstellen zeitnah zu bewerten und zu schließen.

Sie muss nicht jede KI-Anwendung prüfen. Aber sie muss verlangen, dass es eine Inventur, Nutzungsregeln und menschliche Kontrolle gibt.

Führung bedeutet hier nicht Omnipräsenz und Allwissenheit. Führung bedeutet, die richtigen Fragen im richtigen Rhythmus zu stellen und die Antworten nicht im Nebel stehen zu lassen.

Das erste Lagebild

Herr Baumann bekam eine Woche Zeit. Nicht um alle Probleme zu lösen, sondern um ein Lagebild zu erstellen.

Keine Präsentation mit vierzig Folien. Eine klare Übersicht.

Frau Weber schrieb die Punkte auf:

1. Welche Systeme sind kritisch für den Betrieb?
2. Welche Schutzmaßnahmen bestehen wirklich?
3. Welche Maßnahmen sind geplant, aber noch nicht umgesetzt?
4. Welche offenen Risiken sind der IT bekannt?
5. Welche Entscheidungen braucht Baumann von der Geschäftsleitung?
6. Welche Punkte können wir belegen?

Hartmann ergänzte:

| „Und bitte in einer Sprache, die ich verstehe.“

Baumann nickte.

Das war wichtig. Ein Bericht, den die Geschäftsleitung nicht versteht, ist kein Lagebild. Er ist eine Beruhigungsfolie. Fachsprache kann notwendig sein. Aber Führung braucht Übersetzung.

Wenn ein IT-Bericht klingt, als wolle er seine Empfänger beeindrucken, verfehlt er seinen Zweck. Er muss Entscheidungen ermöglichen.

Die Schulbank der Leitung

Am Ende der Sitzung kam der unbequemste Punkt.

„Wenn ich überwachen soll“, sagte Hartmann, „muss ich mehr verstehen.“

„Ja“, sagte Weber.

Das war eine knappe Feststellung. Aber sie traf zu.

Viele Geschäftsleiter besuchen Strategietagungen, Finanzierungsrunden, Steuertermine, Bankgespräche und Führungskräfteworkshops. Bei Cyber-Schulungen schicken sie Mitarbeiter. Das ist nicht mehr ausreichend.

Die Geschäftsleitung braucht ein eigenes Verständnis. Nicht technisch bis in die Tiefe, aber ausreichend, um Risiken einordnen, Berichte bewerten und Entscheidungen treffen zu können.

Eine Schulung der Leitung ist kein Zeichen von Schwäche. Sie ist ein Zeichen von Professionalität.

Wer führen will, muss lernen.

Das gilt im Steuerrecht, im Arbeitsrecht, in der Finanzierung, bei Nachhaltigkeit, bei Nachfolge - und inzwischen auch bei Cyber und KI.

Was Hartmann ändert

Eine Woche später war die Tagesordnung der Geschäftsleitung anders.

Zwischen Liquiditätsplanung, Personal und Investitionen stand ein neuer Punkt:

„Cyber, Datenschutz und KI – Lagebild und Entscheidungen.“

Nicht einmalig. Wiederkehrend.

Baumann bereitete vor. Weber prüfte Nachweise. Hartmann entschied. Der Beirat sollte künftig eine Zusammenfassung erhalten.

Das war noch keine perfekte Sicherheitsorganisation. Aber es war ein Bruch mit dem alten Muster.

Nicht mehr: „Die IT macht das.“

Sondern: „Die IT bereitet vor. Die Leitung führt.“

Das klingt nach einem kleinen Unterschied.

In der Krise kann es der entscheidende sein.

MEMO

1. Wo steht Cybersicherheit in Ihrer Geschäftsleitung tatsächlich auf der Tagesordnung?
2. Gibt es regelmäßige Berichte, die die Leitung versteht?
3. Wer entscheidet über Risikomaßnahmen, Budget, Prioritäten und Restunsicherheiten?
4. Welche Protokollsätze könnten später so wirken, als sei Verantwortung einfach nach unten delegiert worden?
5. Hat die Geschäftsleitung selbst eine Schulung erhalten?
6. Können Sie belegen, dass Maßnahmen nicht nur geplant, sondern überwacht wurden?

Der zweite Irrtum ist damit benannt: Nicht die IT trägt die Gesamtverantwortung. Die IT ist unverzichtbar. Aber Führung bleibt oben.

Und wenn Führung oben bleibt, kommt die nächste Frage zwangsläufig:

Woher wissen wir eigentlich, ob wir betroffen sind?

6 | Es kommt keine Post vom Amt

Thomas Hartmann wartete auf ein Zeichen.

Nicht bewusst. Niemand würde es so formulieren. Aber innerlich erwartete er, dass eine Behörde irgendwann Bescheid geben würde, wenn sein Unternehmen wirklich gemeint war. Ein Schreiben, ein Portalhinweis, eine Registrierungsaufforderung, ein Aktenzeichen. So war man es gewohnt. Das Finanzamt meldete sich. Die Berufsgenossenschaft meldete sich. Der Kunde meldete sich. Irgendjemand meldete sich immer.

Bei Cyber-Pflichten funktioniert dieses Abwarten gefährlich schlecht.

Die neue Lage verlangt von Unternehmen, sich selbst zu prüfen. Branche, Größe, Tätigkeit, Rolle in der Lieferkette, digitale Abhängigkeiten, besondere Dienste, Kundenvorgaben, Versicherungsbedingungen. Das Unternehmen muss nicht erst wichtig aussehen, um prüfen zu müssen. Es muss wissen, ob es in relevante Pflichten hineinläuft.

Hartmann fand das unbefriedigend.

„Sie meinen, ich muss prüfen, ob ich prüfen muss?“

„Ja“, sagte Weber. „Und wir sollten das schriftlich tun“, fügte sie hinzu

Das klang nach Bürokratie. War es aber nicht. Es war der Anfang einer Verteidigungslinie.

Der falsche Trost der Unklarheit

Unklare Rechtslagen haben eine merkwürdige Wirkung. Sie beruhigen kurzfristig.

Solange etwas nicht eindeutig ist, kann man sich einreden, nicht gemeint zu sein. Solange kein Brief kommt, scheint die Lage offen. Solange andere lauter betroffen wirken, kann man hoffen, noch Zeit zu haben.

Aber Unklarheit ist keine Entlastung. Sie ist ein Auftrag zur Klärung.

Gerade Geschäftsführer und Beiräte sollten diesen Unterschied verstehen. In vielen Bereichen des Unternehmens akzeptieren sie ihn längst. Niemand wartet darauf, dass die Bank erklärt, ob Liquidität wichtig ist. Niemand wartet darauf, dass ein Kunde erklärt, ob Qualität zählt. Niemand wartet darauf, dass ein Steuerbescheid kommt, bevor man eine steuerliche Struktur prüft.

Bei Cyber wird trotzdem oft gewartet.

Das ist bequem, aber riskant.

Wenn später ein Kunde, ein Versicherer, eine Aufsicht oder ein Gesellschafter fragt, warum nichts geprüft wurde, hilft der Satz „wir waren uns nicht sicher“ nur begrenzt. Besser ist eine dokumentierte Selbstprüfung: Wir haben Branche, Größe, Tätigkeiten, Konzernstruktur, Kundenanforderungen und Sonderrollen geprüft. Ergebnis: betroffen, nicht betroffen oder weiter zu klären. Maßnahmen: festgelegt. Datum: dokumentiert.

Das ist keine Garantie. Aber es zeigt Führung.

Drei Prüfungen statt einer

Hartmann wollte eine klare Antwort.

| „Sind wir betroffen – ja oder nein?“

Diese Frage ist verständlich. Sie greift aber zu kurz.

Für ein Unternehmen wie Hartmann Maschinenbau sind drei Prüfungen sinnvoll.

Erstens: die rechtliche Betroffenheit. Welche Gesetze, Verordnungen und branchenspezifischen Pflichten gelten unmittelbar? Welche Rolle spielen Mitarbeiterzahl, Umsatz, Bilanzsumme, Sektor, Tätigkeit und Sonderregeln? Diese Prüfung gehört sauber dokumentiert und bei Änderungen aktualisiert.

Zweitens: die wirtschaftliche Betroffenheit. Was verlangen Kunden, Banken, Versicherer, Investoren, Beiräte oder Käufer? Ein

Unternehmen kann wirtschaftlich in der Pflicht stehen, auch wenn die unmittelbare gesetzliche Pflicht im Detail noch diskutiert wird. Wer einen Großkunden verliert, weil er Sicherheitsanforderungen nicht nachweisen kann, hat wenig davon, rechtlich vielleicht knapp außerhalb einer Schwelle zu liegen.

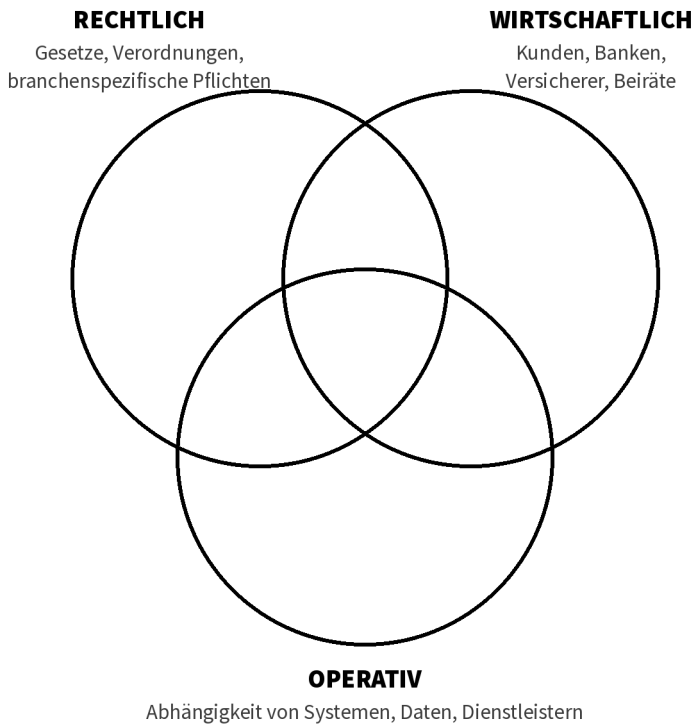
Drittens: die operative Betroffenheit. Wie abhängig ist der Betrieb tatsächlich von digitalen Systemen, Daten, Dienstleistern und KI? Ein Unternehmen kann regulatorisch kleiner wirken, aber operativ hoch verwundbar sein.

Diese drei Prüfungen gehören zusammen.

Ein reiner Gesetzescheck ist zu wenig. Ein reiner IT-Check ist zu wenig. Ein reiner Kundenfragebogen ist zu wenig.

Die Geschäftsleitung braucht ein Gesamtbild.

Betroffenheit: drei Prüfungen statt einer



Betroffenheit durch Gesetze, Kunden und eigene Systeme prüfen.

Der Fragebogen als Warnsignal

Der Kundenfragebogen lag wieder auf dem Tisch.

Hartmann hatte ihn zunächst als lästige Zusatzaufgabe gesehen. Jetzt wurde er zu einem Frühwarnsignal. Jede Frage zeigte eine Erwartung des Kunden.

Haben Sie ein Informationssicherheitskonzept?

Das heißt: Wir wollen wissen, ob Sie Ihr Risiko strukturiert steuern.

Haben Sie Mehr-Faktor-Athentifizierung für externe Zugänge?

Das heißt: Wir wollen nicht, dass ein schlecht gesicherter Zugang Ihr Unternehmen und damit unsere Lieferkette gefährdet.

Wann wurde der letzte Wiederherstellungstest durchgeführt?

Das heißt: Uns interessiert nicht nur, ob Sie ein Backup haben. Uns interessiert, ob Sie im Notfall wieder anlaufen können.

Wie prüfen Sie Dienstleister mit administrativem Zugriff?

Das heißt: Ihr Dienstleister kann zu unserem Problem werden.

Gibt es Schulungen?

Das heißt: Wir wissen, dass Technik allein nicht reicht.

Hartmann las die Fragen anders als am ersten Tag. Nicht mehr als Zumutung. Eher als kostenlose Marktforschung. Der Kunde sagte ihm, was künftig zählt.

Das ist ein Perspektivenwechsel.

Wer Fragebögen nur abarbeitet, bleibt Getriebener. Wer sie auswertet, erkennt Markterwartungen.

Die Selbstprüfung darf nicht im Kopf bleiben

Weber war an diesem Punkt unerbittlich.

„Wir machen eine Akte“, sagte sie.

Hartmann verzog das Gesicht.

„Noch eine?“

„Ja. Eine, die uns später helfen kann.“

Die Akte bekam den Arbeitstitel: Betroffenheits- und Anforderungsprüfung.

Sie enthielt nicht nur eine juristische Einschätzung. Sie enthielt das, was die Geschäftsleitung wirklich wissen musste:

Welche Gesellschaften gehören zur Gruppe?

Welche Tätigkeiten üben sie aus?

Wie viele Mitarbeiter und welche Umsätze sind relevant?

Welche Kunden stellen Sicherheitsanforderungen?

Welche Versicherer verlangen bestimmte Maßnahmen?

Welche Dienstleister haben kritische Zugriffe?

Welche KI-Anwendungen werden genutzt?

Welche offenen Punkte müssen anwaltlich oder fachlich vertieft werden?

Die Akte war nicht perfekt. Aber sie existierte.

Das ist der Unterschied zwischen einem Unternehmen, das hofft, und einem Unternehmen, das prüft.

Der Irrtum der kleinen Gesellschaft

Ein paar Tage später rief Hartmanns Cousin Klaus an. Er war Geschäftsführer der Familienholding.

„Thomas, betrifft uns das auch? Wir haben doch nur drei Leute.“

Hartmann hätte früher wahrscheinlich geantwortet: „Nein, Klaus, natürlich nicht.“

Jetzt sagte er: „Kommt darauf an.“

Das war die bessere Antwort.

Viele Gruppen haben kleine Gesellschaften, die auf dem Papier harmlos wirken: Holding, Immobiliengesellschaft, Verwaltungsgesellschaft, IP-Gesellschaft, Servicegesellschaft. Drei Mitarbeiter, geringe operative Tätigkeit, wenig Außenwirkung.

Aber manchmal haben genau diese Einheiten Schlüssel: zentrale IT-Verträge, Administratorrechte, Gruppenrichtlinien, gemeinsame Datenräume, Konten, Cloud-Zugänge, Versicherungen oder Dienstleisterverträge.

Klein heißt nicht automatisch unwichtig.

Eine kleine Gesellschaft mit zentralem Zugriff kann operativ bedeutsamer sein als eine große Gesellschaft ohne Schlüssel.

Deshalb reicht es nicht, nur auf Köpfe und Umsätze zu schauen. Man muss auch fragen: Wer hält welche Zugänge? Wer steuert welche Systeme? Wer beauftragt welche Dienstleister? Wer sammelt welche Daten? Wer ist im Notfall handlungsfähig?

Keine Panikprüfung

Der Zweck dieser Prüfung ist nicht, jedes Unternehmen in Alarmzustand zu versetzen.

Panik ist ebenso schlecht wie Wegsehen.

Eine gute Selbstprüfung sortiert. Sie unterscheidet zwischen unmittelbarer Pflicht, mittelbarem Druck, freiwilliger Vorsorge und wirtschaftlicher Notwendigkeit. Sie zeigt, was sofort zu tun ist, was geplant werden kann und was nur beobachtet werden muss.

Hartmann lernte dabei eine wichtige Regel:

Nicht jeder roter Signalfarbe markierte offene Punkt ist eine Katastrophe. Aber jeder dieser Punkte braucht eine Zuständigkeit, eine Arbeitsanweisung und eine Frist.

Ohne diese drei Dinge wird aus einer offenen Frage ein vergessenes Risiko.

Memo für die Geschäftsleitung

Am Ende dieses Kapitels steht keine in einem Paragraphen geregelte Feststellung zur rechtlichen Betroffenheitsprüfung, sondern ein weiter gefächelter Arbeitsauftrag.

Die Geschäftsleitung sollte eine Betroffenheits- und Anforderungsprüfung beschließen. Nicht als akademische Übung, sondern als Führungsinstrument.

Dazu gehören mindestens:

MEMO

1. Rechtliche Selbstprüfung: Welche Pflichten können unmittelbar gelten?
2. Kundenprüfung: Welche Anforderungen stellen unsere wichtigsten Kunden?
3. Versicherungsprüfung: Welche Sicherheitsmaßnahmen wurden zugesichert oder verlangt?
4. Lieferantenprüfung: Welche Dienstleister haben kritischen Zugriff?
5. Gruppenprüfung: Welche Gesellschaften, Holdingstrukturen und zentralen Funktionen sind relevant?
6. KI-Prüfung: Welche KI-Werkzeuge sind im Einsatz?
7. Nachweisprüfung: Was können wir belegen?

Diese Prüfung muss nicht alle Antworten sofort liefern. Aber sie muss die offenen Fragen sichtbar machen.

Hartmann hatte anfangs auf Post gewartet.

Jetzt verstand er: Die wichtigste Nachricht kommt nicht immer von außen.

Manchmal muss die Geschäftsleitung sie selbst schreiben.

Und sobald klar ist, dass Handlungsbedarf besteht, folgt die nächste Frage:

Was genau müssen wir eigentlich tun?

Teil III – Die neue Führungsaufgabe

Wie Cyber, KI und Daten zur Chefsache werden

7 | Die zehn Fragen der Geschäftsleitung

IT-Leiter Baumann kam mit einer Liste.

Diesmal nicht mit einer Präsentation, sondern mit zwei Seiten Papier. Die kaufmännische Leiterin hatte darauf bestanden. „Wenn es wichtig ist, muss es auf zwei Seiten verständlich sein“, hatte Weber gesagt.

Oben stand:

Cyber-Risikomanagement – erste Führungsfragen

Hartmann nahm die Liste, las die Überschrift und schaute auf.

„Ich dachte, das sind Maßnahmen.“

„Sind es auch“, sagte Baumann. „Aber wenn ich sie als technische Maßnahmen formuliere, diskutieren wir über Produkte. Wenn ich sie als Fragen formuliere, diskutieren wir über Führung.“

Das war klug.

Denn genau daran scheitern viele Unternehmen: Sie beginnen mit Werkzeugen. Firewall, Endpoint-Schutz, Backup-Lösung, Awareness-Plattform, Dienstleister, Zertifikat. Alles kann sinnvoll sein. Aber ohne die richtigen Führungsfragen wird aus Sicherheit ein Einkaufsvorgang.

Als Geschäftsführer brauchte Hartmann keine Einkaufsliste. Er brauchte eine Struktur.

Frage 1: Welche Risiken tragen wir wirklich?

Die erste Frage klingt einfach.

Welche Risiken bestehen für unser Unternehmen?

Viele Unternehmen beantworten sie zu technisch: Malware, Phishing, Ransomware, DDoS, Datenabfluss. Das sind Angriffsarten. Die Geschäftsleitung muss weiter fragen:

Was bedeutet das für uns?

Welche Produkte könnten nicht geliefert werden? Welche Kunden wären betroffen? Welche Zahlungen könnten nicht ausgeführt werden? Welche Daten wären kritisch? Welche Fristen würden laufen? Welche Verträge würden verletzt? Welche Reputationsschäden wären realistisch?

Risiko ist nicht nur die Wahrscheinlichkeit eines Angriffs. Risiko ist die Wirkung auf das Geschäft.

Für Hartmann war das eine neue Perspektive. Baumann sprach von Systemen. Keller sprach von Produktion. Weber sprach von Liquidität. Der Vertrieb sprach von Kunden. Erst zusammen ergab sich das Risiko.

Frage 2: Was passiert in der ersten Stunde?

Viele Notfallpläne beginnen zu spät.

Sie beschreiben Krisenstab, Kommunikation, externe Experten und Wiederherstellung. Alles wichtig. Aber die erste Stunde entscheidet oft, ob die Krise größer wird.

Wer darf Systeme trennen? Wer darf nicht neu starten? Wer dokumentiert? Wer ruft wen an? Wo liegen Telefonnummern, wenn E-Mail und Adressbuch nicht erreichbar sind? Wer entscheidet, ob Kunden informiert werden? Wer bindet Datenschutz, Rechtsberatung, Forensik und Versicherer ein?

Hartmann merkte: Der Notfallplan lag im System.

Das war ein Problem.

Ein Notfallplan, der nur digital im betroffenen Netz liegt, ist im Notfall kein Plan. Er ist ein unerreichbares Dokument. Er ist Teil des Problems, nicht der Lösung.

Die Geschäftsleitung muss deshalb nicht nur fragen, ob ein Plan existiert. Sie muss fragen, ob er im Ernstfall nutzbar ist.

Frage 3: Können wir wieder anlaufen?

„Wir haben Backups“, sagte Herr Baumann.

| „Wann haben wir zuletzt zurückgespielt?“, fragte Frau Weber.

Das war der Unterschied zwischen Existenz und Wirksamkeit.

Ein Backup ist nur so gut wie die Wiederherstellung. Viele Unternehmen sichern Daten, ohne regelmäßig zu testen, ob ein Wiederanlauf in der nötigen Zeit möglich ist. Im Ernstfall stellt sich dann heraus: Die Sicherung ist unvollständig, zu langsam, ebenfalls verschlüsselt oder technisch nicht in der erwarteten Form nutzbar.

Die Geschäftsleitung muss deshalb zwei Dinge verstehen, ohne sie technisch zu vertiefen:

Wie lange darf ein Prozess ausfallen?

Wie viel Datenverlust kann das Unternehmen verkraften?

Diese Fragen beantwortet nicht die IT allein. Sie betreffen Kunden, Produktion, Liquidität und Verträge. Ein Tag Ausfall kann in einem Bereich tolerierbar sein. In einem anderen kann eine Stunde kritisch sein.

Frage 4: Wer hat Schlüssel zu unserem Haus?

Dienstleister sind unverzichtbar. Cloud-Anbieter, IT-Service, Maschinenwartung, Lohnabrechnung, Website-Agentur, Softwareanbieter, externe Berater. Ohne sie läuft kaum ein modernes Unternehmen.

Aber jeder Dienstleister mit Zugriff ist auch Teil der Risikoland-schaft.

Hartmanns Liste war länger, als er erwartet hatte. Cloud-ERP, Fernwartung, Telefonanlage, Maschinensteuerung, Zeiterfassung, Hosting, Newsletter, Personalsoftware, Steuerberaterportal, externe Entwickler.

Die Frage lautet nicht: Vertrauen wir denen?

Die Frage lautet: Was dürfen sie? Wie sind ihre Zugänge geschützt? Was steht im Vertrag? Wer löscht alte Zugänge? Wer prüft Unterauftragnehmer? Wer wird informiert, wenn dort ein Vorfall passiert?

Vertrauen ist gut. Geregelter Zugriff ist besser.

Frage 5: Wie schließen wir bekannte Schwachstellen?

Baumann erklärte den Patch-Prozess.

Hartmann verstand nicht jedes technische Detail. Das musste er auch nicht. Wichtig war etwas anderes: Es gab Systeme, bei denen Updates schnell möglich waren, und solche, bei denen jede Änderung mit Produktionsrisiken verbunden war.

Alte Maschinen, spezielle Software, produktionsnahe Systeme hier ist Patchen nicht immer einfach. Aber Nichtstun ist keine Strategie.

Wenn ein System nicht aktualisiert werden kann, braucht es andere Maßnahmen: Segmentierung, begrenzte Zugänge, Monitoring, Ersatzplanung, klare Risikodokumentation.

Die Geschäftsleitung muss wissen, wo solche Ausnahmen bestehen. Nicht jede Ausnahme ist falsch. Aber jede Ausnahme braucht eine Begründung und einen Plan.

Frage 6: Funktionieren unsere Maßnahmen wirklich?

Eine Maßnahme ist nicht deshalb wirksam, weil sie beschlossen wurde.

Mitarbeiter können geschult sein und trotzdem nicht wissen, wie sie im Ernstfall reagieren. Backups können laufen und trotzdem nicht wiederherstellbar sein. Zugänge können abgesichert sein, aber alte Konten können offen bleiben. Lieferanten können Fragebögen ausfüllen, ohne dass kritische Punkte geprüft werden.

Wirksamkeit entsteht durch Tests, Übungen, Stichproben und ehrliche Auswertung.

Hartmann mochte das Wort „ehrlich“ in diesem Zusammenhang nicht. Es klang, als hätten sie vorher nicht ehrlich gearbeitet. Weber widersprach.

„Ehrlich heißt nicht, dass vorher jemand gelogen hat. Ehrlich heißt, dass wir zulassen, dass es offene Punkte gibt, die wir so lange rot markieren, bis sie gelöst sind.“

Das ist entscheidend.

Ein Cockpit, in dem alle Lämpchen grün sind, obwohl niemand genau geprüft hat, ist gefährlicher als rot leuchtende Warnsignale. Rot zeigt Handlungsbedarf. Falsches Grün erzeugt Scheinsicherheit.

Frage 7: Wissen unsere Menschen, was zu tun ist?

Schulung ist mehr als Teilnahme.

Eine unterschriebene Liste beweist nicht, dass Menschen handeln können. Sie beweist nur, dass sie anwesend waren oder einen Kurs abgeschlossen haben.

Die Geschäftsleitung muss fragen: Erkennen Mitarbeiter typische Betrugsversuche? Gibt es klare Zahlungsregeln? Wissen Führungskräfte, wie sie mit Verdachtsmeldungen umgehen? Sind neue Mitarbeiter eingebunden? Gibt es Wiederholungen? Werden auch Geschäftsleitung und Beirat geschult?

Cybersicherheit ist Verhaltenssicherheit.

Ein Unternehmen kann technisch gut aufgestellt sein und trotzdem an einer E-Mail scheitern, die Dringlichkeit, Autorität und Vertraulichkeit geschickt kombiniert.

Frage 8: Sind kritische Daten geschützt?

Verschlüsselung klingt technisch. In Wahrheit ist sie ein Führungsinstrument.

Wenn Daten abfließen, macht es einen großen Unterschied, ob sie für Unbefugte lesbar sind. Das betrifft Datenschutz, Kundenvertrauen, Meldepflichten, Erpressungsdruck und Schadenshöhe.

Die Geschäftsleitung muss nicht den Algorithmus kennen. Aber sie sollte wissen, welche Daten besonders sensibel sind, wo sie liegen, wie sie übertragen werden, wer Zugriff hat und ob Schutzmaßnahmen dem Risiko entsprechen.

Nicht alle Daten sind gleich. Aber manche Daten sind Kronjuwelen. Wer seine Kronjuwelen nicht kennt, kann sie nicht schützen.

Frage 9: Wer darf was?

Zugriffsrechte wachsen in Unternehmen wie Schichten von Papierstapeln auf einem alten Schreibtisch.

Ein Mitarbeiter wechselt die Abteilung, behält aber alte Rechte. Ein Dienstleister beendet das Projekt, der Zugang bleibt. Ein Administrator richtet ein Konto ein, das später niemand mehr kennt. Ein temporärer Zugriff wird dauerhaft.

Das ist menschlich. Und riskant.

Die Geschäftsleitung muss deshalb regelmäßige Berechtigungsprüfungen verlangen. Wer hat administrative Rechte? Wer genehmigt sie? Wer überprüft sie? Wie schnell werden ausgeschiedene Mitarbeiter entfernt? Welche externen Konten existieren?

Das Prinzip ist einfach: So viel Zugriff wie nötig. So wenig wie möglich.

Frage 10: Wie kommunizieren wir sicher?

Sichere Kommunikation betrifft nicht nur Verschlüsselung. Sie betrifft auch Verlässlichkeit.

Wie erreichen wir Mitarbeiter, wenn E-Mail ausfällt? Wie informieren wir Kunden? Wer spricht mit Medien? Wie werden geänderte Bankverbindungen geprüft? Wie stellen wir sicher, dass in der Krise keine widersprüchlichen Nachrichten entstehen?

Kommunikation ist im Cybervorfall Teil der Schadensbegrenzung. Schweigen erzeugt Gerüchte. Zu viel Sicherheit in Aussagen erzeugt Haftungsrisiken. Gute Kommunikation sagt, was bekannt ist, was noch geprüft wird und wann die nächste Information kommt.

Aus zehn Fragen wird ein Arbeitsplan

Am Ende der Sitzung waren die zwei Seiten voller handschriftlicher Notizen.

Hartmann hatte verstanden: Die zehn Fragen waren keine einmalige Übung. Sie waren die Struktur eines dauerhaften Führungsprozesses.

Weber schlug vor, daraus eine Maßnahmen-Matrix zu machen – mit einer Zeile je Führungsfrage und Spalten für den aktuellen Status, den Nachweis, den Verantwortlichen, die nächste Maßnahme, den Termin und die Entscheidung der Geschäftsleitung.

Damit wurde aus einem abstrakten Thema ein Steuerungsinstrument.

Nicht perfekt. Aber brauchbar.

Und brauchbar schlägt perfekt, wenn perfekt nur dazu dient, nicht anzufangen.

MEMO

1. Gibt es eine aktuelle Risikoanalyse, die Geschäftsrisiken und nicht nur IT-Risiken beschreibt?
2. Ist die erste Stunde eines Vorfalls geregelt?
3. Wurden Wiederherstellungen tatsächlich getestet?
4. Sind kritische Dienstleister und Zugänge bekannt?
5. Gibt es einen Prozess für Schwachstellen und Ausnahmen?
6. Werden Maßnahmen auf Wirksamkeit geprüft?
7. Sind Mitarbeiter und Leitung geschult?
8. Sind besonders sensible Daten identifiziert und geschützt?
9. Werden Zugriffsrechte regelmäßig überprüft?
10. Gibt es eine sichere Kommunikationslinie für Krise und Alltag?

Hartmann legte die Liste in den roten Ordner.

Nicht, weil der Ordner alles löste.

Sondern weil er zum ersten Mal sah, worüber er führen musste.

Im nächsten Kapitel sollte er lernen, dass nicht alle Schwachstellen der Cybersicherheit mit Servern, Verschlüsselung oder Passwörtern zu tun haben.

Sie können auch einfach am Schreibtisch sitzen. Hilfsbereit sein. Und eine E-Mail mit einfachen Anweisungen bekommen.

8 | Der Mensch öffnet die Tür

Frau Berger machte an diesem Dienstag genau das, wofür man sie seit zweiundzwanzig Jahren schätzte.

Sie kümmerte sich.

In der Buchhaltung war sie eine Institution. Nicht laut, nicht spektakulär, aber verlässlich. Wenn ein Beleg fehlte, fand sie ihn. Wenn eine Zahlung falsch zugeordnet war, merkte sie es. Wenn jemand eine unklare Rechnung auf ihren Tisch legte, kam sie selten mit Meinung zurück, sondern mit Klärung.

Dann kam die E-Mail.

Absender: Thomas Hartmann.

Betreff: Dringend – bitte vertraulich.

Ein italienischer Lieferant brauche heute noch eine Anzahlung. Der Vertrag hänge daran. Die Bankverbindung habe sich geändert. Bitte keine Rückfragen über die normale Buchhaltung, das sei noch nicht spruchreif. „Ich verlasse mich auf Sie.“

Frau Berger las die Mail zweimal.

Der Ton passte. Knapp, direkt, ein wenig ungeduldig. So schrieb Hartmann manchmal, wenn er auf Reisen war oder zwischen Terminen entschied. Der Betrag war hoch, aber nicht undenkbar.

Sie zögerte.

Dieses Zögern war wichtig.

Drei Sekunden, vielleicht vier. Genug Zeit, in der eine gute und klar formulierte Regel hätte greifen können.

Aber es gab keine klare Regel.

Also tat Berger, was pflichtbewusste Menschen tun, wenn sie glauben, gebraucht zu werden.

Sie half.

Der Angriff auf die Hilfsbereitschaft

Später saß die Buchhalterin im kleinen Besprechungsraum. Vor ihr stand ein Glas Wasser. Sie fasste es nicht an.

Hartmann stand am Fenster. Er war nicht in Italien gewesen. Er hatte keine Zahlung angewiesen. Der Lieferant existierte, aber nicht diese Bankverbindung. Das Geld war unterwegs.

„Ich dachte, Sie sind das“, sagte Berger.

Hartmann nickte.

„Ich weiß.“

Dieser Satz war wichtig. Er verhinderte, dass aus einem Vorfall ein Kulturbruch wurde.

Denn nicht die Buchhalterin war das Problem. Sie war nicht dumm. Sie war nicht nachlässig. Sie war loyal, erfahren und hilfsbereit. Genau diese Eigenschaften waren ausgenutzt worden.

Moderne Angriffe zielen nicht nur auf technische Schwächen. Sie zielen auch auf menschliche Muster: Vertrauen, Dringlichkeit, Autorität, Hilfsbereitschaft, Angst vor Fehlern, Wunsch nach Diskretion.

„Dringend.“

„Vertraulich.“

„Ich verlasse mich auf Sie.“

Soche Formulierungen durchbrechen keine Firewall. Aber in Unternehmen ohne schützende Vorschriften öffnen sie trotzdem Türen. Und können damit größeren Schaden anrichten als ein schlechtes Passwort.

Schuldzuweisung vergrößert das Problem

Viele Unternehmen reagieren nach einem solchen Vorfall falsch. Sie suchen eine Person, nicht ein Muster.

Wer hat geklickt? Wer hat überwiesen? Wer hat nicht gefragt? Wer war schuld?

Natürlich muss ein Vorfall aufgearbeitet werden. Natürlich muss man verstehen, was passiert ist. Aber wer den Menschen vorführt, statt den Prozess zu prüfen, macht das Unternehmen unsicherer.

Der nächste Mitarbeiter wird dann nicht schneller melden. Er wird schweigen, hoffen, vertuschen, später berichten. Genau das ist gefährlich.

Eine gute Sicherheitskultur macht Melden leicht und Beschämung schwer.

Hartmann entschied richtig. Er stellte Frau Berger nicht an den Pranger. Er legte den Prozess offen auf den Tisch.

Warum war eine Zahlung dieser Höhe ohne zweite Bestätigung möglich?

Warum gab es keine feste Rückrufregel bei geänderten Bankverbindungen?

Warum konnte „vertraulich“ eine normale Kontrolle außer Kraft setzen?

Warum wusste niemand, welche Formulierungen typisch für Betrugsversuche sind?

Warum war es nicht ausdrücklich erlaubt, auch dem Chef gegenüber zu sagen: „Ich prüfe das.“

Das waren die richtigen Fragen.

Der Prozess war die Schwachstelle

Die Rekonstruktion war nüchtern.

Eingang der Mail: 13:28 Uhr.

Freigabe: 13:41 Uhr.

Überweisung: 13:49 Uhr.

Einundzwanzig Minuten.

Kein Server war verschlüsselt. Keine Firewall war durchbrochen. Kein Angreifer hatte sich durch das Netzwerk bewegt. Der Schaden entstand durch einen ordentlichen Zahlungsprozess.

Nur war der Prozess nicht sicher genug.

Das ist für viele Unternehmer schwer zu akzeptieren. Cyber wird mit Angriffen auf Systeme verbunden. Aber ein digital ausgelöster Vermögensschaden kann entstehen, ohne dass ein technischer Einbruch nachweisbar ist. Social Engineering nutzt Organisation, Kommunikation und Kultur.

Deshalb helfen nicht nur bessere Filter. Sie helfen, aber sie reichen nicht.

Was gebraucht wird, sind Regeln, die Menschen unter Druck entlasten.

Eine klare Regel ist kein Misstrauen. Sie ist Schutz.

Wenn jede neue Bankverbindung über eine bekannte Telefonnummer bestätigt werden muss, muss Buchhalterin Berger nicht entscheiden, ob sie Chef Hartmann misstraut. Die Regel entscheidet für sie.

Wenn Beträge ab einer Schwelle ein Vier-Augen-Prinzip brauchen, ist Nachfragen kein persönlicher Affront. Es ist Standard.

Wenn „vertraulich“ niemals bedeutet, Kontrollen zu umgehen, verliert ein Angreifer eine gefährliche Waffe.

Schulung ist kein Ereignis

Baumann schlug eine Schulung vor.

| „Einmal für alle“, sagte er.

Weber hob den Blick.

| „Einmal reicht nicht.“

Sie hatte recht.

Schulung ist kein Ereignis, das man abhakt. Sie ist ein wiederkehrender Aufbau von Reflexen. Menschen sollen nicht jede Angriffstechnik auswendig kennen. Sie sollen bei bestimmten Mustern innerlich anhalten:

Ungewöhnliche Dringlichkeit.

Geänderte Bankverbindung.

Vertraulichkeit mit Kontrollverbot.

Anhang von unbekannter Quelle.

Link mit Zeitdruck.

Anruf mit künstlicher Autorität.

KI-gestützte Texte machen die Sache schwieriger. Früher waren schlechte Sprache, falsche Umlaute oder seltsame Anreden Warnzeichen. Heute kann ein Betrugstext gut klingen. Sehr gut sogar. Er kann freundlich, präzise und im richtigen Ton geschrieben sein.

Inzwischen kann auch eine künstlich generierte Stimme täuschend echt wirken.

Deshalb darf Schulung nicht nur erklären, woran man schlechte Mails erkennt. Sie muss erklären, welche Prozesse immer gelten, auch wenn die Nachricht gut aussieht.

Die Führung muss mitlernen

Hartmann wollte die Schulung zunächst für die Belegschaft ansetzen.

Weber sagte: „Dann fangen wir bei uns an.“

Das war unbequem. Aber richtig.

Wenn die Geschäftsleitung Sicherheitsregeln nur für andere formuliert, entstehen Lücken. Der Chef selbst ist oft ein beliebtes Angriffsziel. Seine Stimme, sein Stil, seine Autorität, seine Abwesenheit, sein Zeitdruck – all das kann missbraucht werden.

Außerdem beobachten Mitarbeiter sehr genau, ob Regeln auch oben gelten.

Wenn Hartmann selbst Rückrufregeln als lästig behandelt, werden andere sie umgehen. Wenn er Nachfragen als Störung empfindet, wird niemand fragen. Wenn er öffentlich sagt, dass Buchhalterin Berger richtig gehandelt hat, indem sie den Vorfall sofort meldete, verändert das die Kultur.

Sicherheit beginnt nicht in der Schulungsplattform.

Sie beginnt im Verhalten der Führung.

Den Überblick behalten

Drei Wochen später lagen auf dem Besprechungstisch verschiedene Listen.

Herr Baumann hatte die erste Mitarbeiterschulung zu Cyber-schutz-Awareness organisiert und legte die Übersicht über die Teilnehmer vor. Auch eine Auflistung derjenigen, die den Kurs verpasst hatten. Frau Weber hatte parallel dazu Angebote für eine Schulung der Führungskräfte eingeholt. Aus dem Vertrieb kam außerdem die Bitte, zusätzlich zum Awareness-Kurs an einer Einführung zur Nutzung von KI-Werkzeugen teilnehmen zu dürfen. Handschriftlich hatten sich einzelne Mitarbeiter in eine Tabelle eingetragen, um ihr Interesse zu bekunden.

An sich war das eine gute Nachricht. Vor wenigen Wochen hatte niemand über Schulungen gesprochen. Jetzt wollten alle etwas tun.

Frau Weber legte die Listen nebeneinander.

Hartmann wollte Überblick: Wissen wir, welche Schulungen für welche unserer Mitarbeiter gesetzlich vorgeschrieben sind? Und was die Anforderungen der Versicherung sind?

Schweigen.

Hartmann nahm einen der ausgedruckten A4-Bögen in die Hand. Er dachte nach.

Weber zeichnete die Spalten einer Tabelle.

Name des Mitarbeiters.

Awareness-Schulung: vorgeschrieben Ja / Nein, vorgesehen für, absolviert am ...

Einführung KI, erwünscht?

Baumann schaute skeptisch.

„Was machen wir mit neuen Mitarbeitern?“

„Und denen, die einen Kurs verpassen?“

„Wie erfahren wir, ob neue Schulungen vorgeschrieben sind?“

Hartmann blickte aus dem Fenster.

Vor der Halle fuhr ein Lkw vom Hof, Mitarbeiter trafen ein zum Beginn der nächsten Schicht. Der getrennte Müll wurde abgeholt.

Alles wirkte geordnet.

Das Thema Schulungen nicht.

„Fragen wir uns einmal ehrlich“, sagte er. „Wenn morgen unser Versicherer wissen möchte, welche Mitarbeiter innerhalb der letzten zwölf Monate in einem bestimmten Thema geschult wurden – könnten wir ihm das innerhalb einer Stunde beantworten?“

„Nein“, erwiderte Weber.

Baumann, sonst in solchen Momenten eher schweigsam, warf ein: „Wir betrachten Schulungen im Moment als Veranstaltungen.“ Und er fügte hinzu: „Dabei sind sie Prozess.“

Hartmann und Weber schauten den IT-Leiter an, erst verwundert, dann erwartungsvoll.

Baumann fuhr fort: „Für unsere Maschinen haben wir ein klares Protokoll. Zustand, Checks, vorgeschriebene Wartungen. Rechtliche Vorschriften, Verantwortlichkeiten, Berichte. Alles wird automatisch und übersichtlich in einem Programm dokumentiert.“

„Menschen sind keine Maschinen“, stellte Weber klar. „Aber es stimmt, die Übersicht müsste dieselbe sein.“

„Dann suchen wir jetzt einen Anbieter, der uns alle Schulungen samt Übersichtssoftware als Gesamtpaket liefert“, entschied Hartmann.

„Mit Erinnerungen, Ablaufdaten, gespeicherten Nachweisen und Zertifikaten. Mit automatischer Aufnahme neuer Mitarbeiter.“

Awareness und Schulung schützen vor Angriffen.

KI-Kompetenz macht konkurrenzfähig.

Aber nur die Übersicht und Ordnung hilft auch beim Nachweis gegenüber Behörden und Versicherung.

Vom Opfer zur Botschafterin

Außerdem veranstaltete Hartmann Maschinenbau zwei Wochen später auch eine intern organisierte Schulung. Frau Berger erzählte, was passiert war.

Nicht jedes Detail. Nicht beschämend. Aber klar.

Sie sagte einen Satz, den niemand vergaß:

„Ich habe nicht überwiesen, weil ich unvorsichtig war. Ich habe überwiesen, weil ich helfen wollte.“

Damit veränderte sie die Stimmung im Raum.

Plötzlich ging es nicht mehr um dumme Fehler. Es ging um die Frage, wie ein Unternehmen seine hilfsbereiten Menschen schützt.

Das ist die richtige Perspektive.

Mitarbeiter sind nicht die Firewall aus Fleisch und Blut. Sie sind Menschen. Menschen brauchen Regeln, Werkzeuge, Übung und die Erlaubnis, im Zweifel zu stocken und nachzufragen.

Der neue Zahlungsprozess

Am Ende der Aufarbeitung standen keine großen Worte, sondern klare Regeln.

1. Geänderte Bankverbindungen werden immer über bekannte Kontaktdaten bestätigt.
2. Zahlungen ab definierter Höhe brauchen ein Vier-Augen-Prinzip.
3. Vertraulichkeit darf Kontrollregeln nicht außer Kraft setzen.
4. Verdachtsfälle werden sofort gemeldet, ohne Schuldvorwurf.
5. Führungskräfte bestätigen schriftlich, dass Nachfragen erwünscht sind.
6. Simulationen und Kurzschulungen werden regelmäßig wiederholt.

Diese Regeln waren nicht kompliziert.

Genau deshalb waren sie gut.

Gute Sicherheitsregeln müssen in den Arbeitstag passen. Wenn sie nur auf dem Papier funktionieren, werden sie umgangen.

Wenn sie zu kompliziert sind, entstehen Schattenprozesse. Wenn sie zu weich sind, helfen sie nicht.

Der beste Prozess ist der, den ein Mensch unter Druck noch anwenden kann.

MEMO

1. Gibt es klare Rückrufregeln bei Zahlungsänderungen?
2. Gibt es ein Vier-Augen-Prinzip für kritische Vorgänge?
3. Ist eindeutig formuliert, dass Dringlich- und Vertraulichkeit niemals Kontrolle außer Kraft setzen dürfen?
4. Wissen Mitarbeiter, wo sie Verdachtsfälle melden?
5. Werden Meldungen gelobt statt bestraft?
6. Nimmt die Geschäftsleitung selbst an Schulungen teil?
7. Werden neue Risiken durch KI-gestützte Täuschung berücksichtigt?
8. Werden Mitarbeiter in ihrem Bedürfnis nach Schulungen gefördert?
9. Werden Schulungen als Veranstaltungen behandelt oder als fortlaufender Prozess verstanden und entsprechend dokumentiert?

Hartmann hatte verstanden: Die teuerste Sicherheitslücke ist nicht der Mensch.

Es ist der Prozess, der den Menschen allein lässt.

Und während die Buchhaltung neue Regeln bekam, wuchs an anderer Stelle ein Risiko, das zunächst modern und harmlos wirkte.

Im Vertrieb schrieb eine Maschine mit.

9 | KI im Giftschränk

Herr Vogel aus dem Vertrieb war stolz.

Er hatte ein Angebot für einen skandinavischen Kunden vorbereitet. Schnell, sprachlich sauber, technisch überzeugend. Früher hätte er für die erste Fassung einen halben Tag gebraucht. Diesmal waren es vierzig Minuten.

| „Die KI hat das wirklich gut gemacht“, sagte er.

Hartmann sah auf.

| „Welche KI?“

Herr Vogel lächelte noch, aber das Lächeln wurde vorsichtiger.

| „Na, das Tool, das wir für Texte nutzen. Für Angebote, Übersetzungen, Zusammenfassungen. Einige Kollegen verwenden es auch.“

| „Einige?“

| „Ich weiß nicht genau, wer alles.“

Damit war das Thema auf dem Tisch.

Nicht als Zukunftsfrage. Nicht als Strategiepapier. Sondern als gelebter Alltag.

KI ist schon im Unternehmen

Viele Geschäftsleitungen sprechen über KI, als läge sie noch vor ihnen.

In Wahrheit ist sie oft schon da.

Nicht immer als offizielles Projekt. Nicht mit Budget, Lenkungs-kreis und Beschluss. Sondern leise: im Browser, in einer App, in einer Übersetzungsfunktion, in einem Chatbot, in einem CRM-Zusatz, in einer Präsentationshilfe, in einer Suchfunktion.

Mitarbeiter nutzen KI, weil sie hilft. Sie formuliert, übersetzt, strukturiert, verdichtet, erklärt, korrigiert und beschleunigt. Das

ist nicht schlecht. Im Gegenteil: Richtig eingesetzt kann KI ein erheblicher Produktivitätsgewinn sein.

Aber unregelte KI ist kein Fortschritt. Sie ist ein blinder Fleck.

Hartmann verstand das schnell, als Weber die ersten Fragen stellte:

Welche Daten wurden eingegeben?

Wurden Kundennamen verwendet?

Wurden Preise, technische Spezifikationen oder Vertragsinhalte kopiert?

Speichert der Anbieter Eingaben?

Wer prüft die Ergebnisse?

Darf ein KI-Text ungeprüft an Kunden gehen?

Gibt es eine Liste der genutzten Werkzeuge?

Niemand konnte alle Fragen beantworten.

Das war die eigentliche Nachricht.

Das Problem ist nicht die KI. Das Problem ist die Ungeregeltheit.

Hartmann neigte zunächst dazu, das Werkzeug zu verbieten.

| „Dann schalten wir das eben ab.“

Das war verständlich. Aber zu kurz gedacht.

Verbote wirken nur, wenn sie realistisch sind. Ein pauschales KI-Verbot kann dazu führen, dass Nutzung nicht verschwindet, sondern unsichtbar wird. Dann hat die Geschäftsleitung nicht weniger Risiko, sondern weniger Kenntnis.

Der bessere Weg ist Ordnung.

Welche KI-Anwendungen sind erlaubt?

Für welche Zwecke?

Mit welchen Daten?

Unter welchen Prüfregelein?

Wer darf neue Werkzeuge freigeben?

Was ist ausdrücklich verboten?

Wann muss Rechts-, Datenschutz- oder Fachprüfung eingebunden werden?

KI braucht kein Klima der Angst. Sie braucht ein Betriebssystem der Verantwortung.

Halluzinationen: Ton sicher, Inhalt schwach

Der skandinavische Kunde meldete sich zwei Tage später.

Eine technische Zusicherung im Angebot sei nicht haltbar. Sie klinge eindeutig, aber sie passe nicht zur Maschine.

Herr Vogel wurde blass.

Die KI hatte eine Formulierung vorgeschlagen. Er hatte sie übernommen. Sie klang gut. Zu gut.

Genau darin liegt eines der Risiken.

KI kann sehr überzeugend formulieren, auch wenn der Inhalt falsch, unvollständig oder unzulässig ist. Der Text wirkt professionell. Die Sprache gibt Sicherheit. Aber Sprache ist kein Nachweis.

Für ein Unternehmen kann das gefährlich werden. Eine falsche technische Zusicherung, eine ungenaue Vertragsformulierung, eine unzulässige Aussage im Marketing oder eine fehlerhafte Auskunft an Kunden kann Folgen haben.

Deshalb braucht KI immer eine Regel:

Die Maschine formuliert. Der Mensch verantwortet.

Wer im Namen des Unternehmens kommuniziert, kann die Verantwortung nicht an ein Werkzeug abgeben.

„Das hat die KI geschrieben“ ist keine Entlastung gegenüber Kunden.

Es ist ein Eingeständnis, dass niemand geprüft hat.

Daten hinein, Risiko heraus

Noch kritischer ist die Frage, was in ein KI-System eingegeben wird.

Viele Nutzer denken bei KI an Ausgabe: Was schreibt sie? Was schlägt sie vor? Welche Antwort liefert sie?

Die wichtigere Frage lautet oft: Was bekommt sie von uns?

Kundendaten, Vertragsentwürfe, interne E-Mails, Preislisten, technische Zeichnungen, Personaldaten, Streitfälle, Steuerinformationen, vertrauliche Präsentationen, Notizen aus Beiratssitzungen ...

Nicht jedes KI-Werkzeug darf solche Daten sehen. Nicht jeder Anbieter ist geeignet. Nicht jede Eingabe ist datenschutzrechtlich, vertraglich oder unternehmensstrategisch unproblematisch.

Hartmann fragte Herrn Vogel:

„Haben Sie Kundendaten eingefügt?“

„Nur den Namen und die Anforderungen“, antwortete Vogel.

„Und technische Details?“

„Ja, aber nichts Geheimes.“

Das ist ein gefährlicher Satz.

Was „geheim“ ist, entscheidet nicht der einzelne Mitarbeiter im Moment der Arbeitserleichterung. Es muss vorher geregelt sein.

Der Chatbot auf der Website

Am selben Tag entdeckte Frau Weber einen Chat-Assistenten auf der Unternehmenswebsite.

„Seit wann haben wir den?“

Der Marketingdienstleister hatte ihn eingebunden. Standardlösung. Modern. Effizient. Entlastet den Vertrieb.

Der Assistent begrüßte Besucher freundlich. Er antwortete auf Fragen zu Produkten, Lieferzeiten und Kontaktwegen. Er klang

menschlich genug, dass nicht jeder Besucher sofort erkennen musste, ob eine Maschine antwortete.

Damit war ein weiteres Thema geöffnet: Transparenz.

Wenn eine Maschine im Namen des Unternehmens kommuniziert, muss das Unternehmen wissen, wann und wie dies kenntlich zu machen ist. Es muss wissen, welche Antworten der Assistent geben darf. Es muss verhindern, dass falsche Zusagen entstehen. Es muss prüfen, ob personenbezogene Daten verarbeitet werden. Es muss regeln, wann ein Mensch übernehmen muss.

| „Das hat der Dienstleister eingerichtet“, sagte jemand.

Hartmann antwortete diesmal schneller:

| „Dann hat er es für uns eingerichtet. Verantwortlich sind wir.“

Das war der richtige Satz.

Die KI-Inventur

Frau Weber schlug eine KI-Inventur vor.

Nicht als großes theoretisches Projekt. Als einfache Bestandsaufnahme:

Welche KI-Werkzeuge werden genutzt?

Wer nutzt sie?

Für welche Zwecke?

Welche Daten werden eingegeben?

Welche Ergebnisse gehen nach außen?

Welche Anbieter stehen dahinter?

Welche Verträge oder Einstellungen gelten?

Welche Risiken bestehen?

Welche Regeln fehlen?

Die erste Inventur war ernüchternd.

Es gab mehr Nutzung als gedacht. Einige Tools waren offiziell, andere nicht. Manche waren in bestehende Software eingebaut. Andere liefen über private oder kostenlose Zugänge. Manche Mitarbeiter waren unsicher, ob eine Funktion überhaupt KI war.

Diese Unsicherheit ist typisch.

Deshalb muss die Geschäftsleitung nicht nur nach „KI-Projekten“ fragen. Sie muss nach KI-Funktionen im Alltag fragen.

KI-Kompetenz ist Führungsaufgabe

Menschen, die KI nutzen, brauchen Kompetenz.

Nicht im Sinne eines Informatikstudiums. Aber sie müssen verstehen, was KI kann, was sie nicht kann, welche Daten problematisch sind, warum Ergebnisse geprüft werden müssen und wann ein Mensch entscheiden muss.

Das gilt für Mitarbeiter. Es gilt aber auch für die Geschäftsleitung.

Hartmann musste nicht lernen, wie ein großes Sprachmodell trainiert wird. Aber er musste lernen, welche Unternehmensrisiken entstehen, wenn KI ungeregelt in Angeboten, HR-Prozessen, Kundenkommunikation oder Entscheidungsunterstützung eingesetzt wird.

KI-Kompetenz ist deshalb nicht nur Schulung. Sie ist Teil der Führungsfähigkeit.

Die ersten Regeln

Am Ende der Woche beschloss Hartmann Maschinenbau eine erste KI-Richtlinie. Sie war bewusst kurz.

1. Keine vertraulichen Kunden-, Personal-, Vertrags- oder Geschäftsgeheimnisse in nicht freigegebene KI-Werkzeuge.
2. KI-Ergebnisse, die nach außen gehen, werden fachlich geprüft.
3. Technische, rechtliche, steuerliche oder vertragliche Aussagen dürfen nicht ungeprüft übernommen werden.
4. Neue KI-Werkzeuge brauchen Freigabe.

5. Chatbots und Assistenten werden transparent gemacht und überwacht.
6. Die KI-Inventur wird regelmäßig aktualisiert.
7. Mitarbeiter erhalten kurze, praktische Schulungen.

Das war noch kein perfektes KI-Governance-System. Aber es war ein Anfang.

Und vor allem: Die Nutzung war nicht länger unsichtbar.

MEMO

1. Welche KI-Werkzeuge werden im Unternehmen genutzt?
2. Welche Daten werden eingegeben?
3. Welche Ergebnisse gehen an Kunden, Mitarbeiter oder Dritte?
4. Wer prüft KI-Ergebnisse fachlich?
5. Gibt es verbotene Eingaben und klare Freigaben?
6. Sind Chatbots und maschinelle Kommunikation erkennbar geregelt?
7. Haben Mitarbeiter und Leitung ausreichende KI-Kompetenz?

Hartmann hatte anfangs geglaubt, KI sei ein Werkzeug des Vertriebs.

Jetzt verstand er: KI ist ein Querschnittsthema der Unternehmensführung.

Und wer die eigenen Werkzeuge nicht kennt, kennt auch seine Risiken nicht.

Im nächsten Kapitel sollte er lernen, dass Risiken nicht an der eigenen Werkstür enden.

10 | Lieferkette: Die offene Seitentür

Der alte Fernwartungszugang gehörte zu Linie drei.

Die Maschine war nicht schön. Sie war auch nicht neu. Aber sie verdiente Geld. Seit Jahren lief sie zuverlässig, mit dieser stillen Würde alter Technik, die niemand fotografiert und jeder vermisst, wenn sie steht.

An der Schaltschranktür klebte ein vergilbter Zettel. Name des Dienstleisters. Telefonnummer. Ein Benutzerhinweis, halb ausgeblichen.

Keller sah den Zettel an.

| „Der hängt da ewig.“

Baumann sagte: „Genau das ist das Problem.“

Nicht alles, was lange funktioniert, ist sicher. Manchmal ist es nur lange nicht aufgefallen.

Unternehmensgrenze ist nicht Risikogrenze

Viele Unternehmer denken in Werksgrenzen. Das Unternehmen beginnt am Tor und endet am Tor. Innen ist man zuständig. Außen sind andere zuständig.

Digital stimmt das nicht mehr.

Daten, Systeme, Zugänge und Abhängigkeiten laufen über Unternehmensgrenzen hinweg. Cloud-Anbieter betreiben Anwendungen. Dienstleister warten Maschinen. Steuerberater, Lohnbüros, Marketingagenturen, Softwareanbieter, Rechenzentren und externe Entwickler verarbeiten Daten oder halten Zugänge. Kunden stellen Portale bereit. Lieferanten verbinden sich mit Systemen.

Die Lieferkette ist nicht mehr nur Materialfluss.

Sie ist auch Datenfluss, Zugriffsfluss und Verantwortungsfluss.

Hartmann sah das Organigramm des Unternehmens an. Es zeigte Geschäftsleitung, Produktion, Vertrieb, Einkauf, Verwaltung. Es sah geordnet aus. Dann legte Baumann eine zweite Karte daneben: Systeme und externe Zugriffe.

Die zweite Karte war unruhiger.

ERP-Cloud. Maschinenwartung. VPN. Lohnabrechnung. Website. Newsletter. Zeiterfassung. CRM. Datenaustausch mit Kunden. Dienstleisterkonto. Externe Backuplösung. KI-Tool. Steuerberaterportal.

„Das ist unser Unternehmen?“, fragte Hartmann.

„Das ist der digitale Teil davon“, sagte Baumann.

Dienstleister sind keine Nebensache

Ein Dienstleister kann zuverlässig, freundlich und fachlich gut sein – und trotzdem ein Risiko darstellen.

Das ist kein Misstrauen. Es ist Realismus.

Wenn ein Dienstleister administrativen Zugriff hat, kann sein Problem Ihr Problem werden. Wenn seine Zugangsdaten kompromittiert werden, stehen Angreifer möglicherweise in Ihrem Haus. Wenn er einen Vorfall zu spät meldet, laufen Ihre Fristen.

Wenn er Unterauftragnehmer einsetzt, von denen niemand weiß, entstehen neue Wege.

Die richtige Frage lautet nicht: Ist der Dienstleister nett?

Die richtige Frage lautet: Ist der Zugriff geregelt?

Wer darf hinein?

Wann?

Wozu?

Mit welchem Schutz?

Mit welcher Protokollierung?

Wie wird der Zugang beendet?

Was passiert bei einem Vorfall?

Wer informiert wen?

Hartmann musste feststellen, dass einige Antworten nicht dokumentiert waren.

Der Fernwartungszugang

Linie drei wurde zum Lehrstück.

Der Fernwartungsdienstleister hatte vor Jahren einen Zugang eingerichtet. Für schnelle Hilfe. Für Störungen am Wochenende. Für Produktionssicherheit.

Das war damals vernünftig.

Aber niemand hatte den Zugang regelmäßig überprüft. Niemand wusste genau, wann er zuletzt genutzt wurde. Niemand hatte sauber dokumentiert, ob ein zweiter Faktor aktiv war. Niemand wusste, ob alte Konten noch bestanden.

Der Zugang war nicht entstanden, weil jemand fahrlässig sein wollte.

Er war entstanden, weil Arbeit erledigt werden musste.

Viele Risiken entstehen so. Nicht durch böse Entscheidung, sondern durch praktische Lösungen, die nie wieder auf den Prüfstand kommen.

Deshalb braucht Lieferkettensicherheit nicht nur neue Verträge. Sie braucht regelmäßige Rückfragen.

Der Kunde als Prüfer

Während Hartmann seine Dienstleister prüfte, prüfte sein Kunde ihn.

Das war die andere Seite der Lieferkette.

Für den großen Kunden war Hartmann Maschinenbau nicht nur Lieferant. Er war Teil der eigenen Stabilität. Wenn Hartmann nicht

liefern konnte, konnte beim Kunden ein Prozess ins Stocken geraten. Wenn Hartmann kompromittiert wurde, konnte er zum Einfallstor für Kommunikation, Daten oder Systeme werden.

Das erklärt, warum Kunden zunehmend fragen.

Nicht aus Schikane. Aus Eigenschutz.

Ein Lieferant, der seine Risiken nicht kennt, ist für einen großen Kunden schwer kalkulierbar. Ein Lieferant, der antworten kann, Nachweise liefert und Vorfälle geordnet behandelt, wird verlässlicher.

Hartmann begann zu verstehen: Er war nicht nur Opfer möglicher Anforderungen. Er konnte daraus einen Vorteil machen.

Sicherheit als Lieferfähigkeit

In der Produktion verstand jeder den Begriff Lieferfähigkeit.

Ein Unternehmen, das nicht liefern kann, verliert Vertrauen. Egal, ob der Grund Materialmangel, Maschinenstillstand oder Ransomware ist. Der Kunde sieht zunächst das Ergebnis: Die Lieferung kommt nicht.

Cybersicherheit ist deshalb Teil der Lieferfähigkeit.

Nicht als Schlagwort. Ganz praktisch.

Wenn ERP und Versand stehen, kommt keine Ware raus.

Wenn Konstruktionsdaten nicht verfügbar sind, kann nicht gefertigt werden.

Wenn ein Dienstleister ausfällt, steht vielleicht ein Prozess.

Wenn Kundeninformationen nicht erreichbar sind, stockt Kommunikation.

Wenn ein Angriff Datenabfluss verursacht, wird Vertrauen beschädigt.

Wer Cyber als Lieferfähigkeit versteht, holt das Thema aus der IT-Ecke. Dann betrifft es Vertrieb, Einkauf, Produktion, Recht, Versicherung, Kommunikation und Geschäftsleitung.

Die Lieferantenakte

Frau Weber schlug eine Lieferantenakte für kritische Dienstleister vor.

Nicht für jeden Büromateriallieferanten. Nicht für jede Kleinigkeit. Für diejenigen, die Zugriff auf Systeme, Daten oder kritische Prozesse haben.

Die Akte enthielt:

Vertrag und Leistungsbeschreibung

Art des Zugriffs

verantwortlicher Ansprechpartner

Sicherheitsanforderungen

Nachweise oder Selbstauskünfte

Unterauftragnehmer, soweit relevant

Meldepflichten bei Vorfällen

Protokollierung und Zugriffsbeschränkung

Datum der letzten Prüfung

offene Maßnahmen

Herr Baumann fand das zunächst bürokratisch.

Dann suchte er die Informationen zum Fernwartungszugang von Linie drei zusammen.

Nach einer Stunde sagte er: „Vielleicht ist eine Akte doch schneller.“

Dokumentation ist oft erst dann lästig, wenn sie fehlt.

Vertragsklauseln reichen nicht

Der Anwalt schickte später eine Musterklausel zur Informationssicherheit.

Hartmann war erleichtert.

„Dann nehmen wir das in alle Verträge auf.“

„Ja“, sagte Weber, „aber damit ist das Thema nicht abgeschlossen.“

Eine Klausel ist wichtig. Aber sie ersetzt keine Prüfung. Papier kann Zusagen festhalten. Es überwacht sie nicht.

Ein Dienstleister kann vertraglich verpflichtet sein und trotzdem unsicher arbeiten. Ein Fragebogen kann ordentlich ausgefüllt sein und trotzdem Lücken verdecken. Ein Zertifikat kann helfen, aber nur im passenden Geltungsbereich.

Die Geschäftsleitung muss deshalb verstehen: Verträge sind Teil der Steuerung, nicht die Steuerung selbst.

Wenn Ihr Problem beim Kunden ankommt

Hartmann stellte sich erstmals die Lieferkette aus Sicht seiner Kunden vor.

Bisher hatte er gedacht: Wenn wir ein Problem haben, müssen wir es lösen. Jetzt verstand er: Wenn sein Problem die Lieferfähigkeit gefährdet, wird es zum Problem des Kunden. Wenn Daten betroffen sind, wird es vielleicht zum Problem weiterer Beteiligter. Wenn Kommunikation ausfällt, entsteht Unsicherheit in der Kette.

Das macht Cyber zu einem Beziehungsthema.

Ein Kunde verzeiht eher einen Vorfall als schlechte Vorbereitung, widersprüchliche Kommunikation oder fehlende Transparenz.

Niemand erwartet, dass ein Lieferant unverwundbar ist. Aber jeder erwartet, dass er professionell handelt.

MEMO

1. Welche Dienstleister haben Zugriff auf Systeme, Daten oder kritische Prozesse?
2. Sind externe Zugänge technisch geschützt, zeitlich begrenzt und protokolliert?
3. Gibt es eine Lieferantenakte für kritische Dienstleister?
4. Welche Sicherheitsanforderungen stellen unsere wichtigsten Kunden?
5. Können wir diese Anforderungen belegen?
6. Gibt es Meldewege, wenn ein Dienstleister einen Vorfall hat?
7. Werden alte Zugänge regelmäßig entfernt?

Hartmann ließ den Zugang von Linie drei nicht einfach löschen. Baumann sicherte Beweise, klärte die Nutzung, begrenzte den Zugriff und stellte auf ein neues Verfahren um.

Das war weniger spektakulär als ein großer Sicherheitskauf.

Aber es war Führung.

Und mit jeder geschlossenen Seitentür wurde deutlicher, was auf dem Spiel stand, wenn trotzdem etwas passierte.

Dann würde es nicht nur um Technik gehen.

Dann würde es um Haftung gehen.

Teil IV – Die Folgen

Was Krise, Haftung und Versicherung wirklich bedeuten

11 | Haftung: Aus Technik wird Verantwortung

Das Wort fiel in einem Raum, in dem niemand es hören wollte.

Innenhaftung.

Thomas Hartmann saß mit seiner Schwester Carola am Konferenztisch. Carola führte den Beirat der Familiengruppe. Sie war keine operative Geschäftsführerin, aber sie kannte das Unternehmen, die Familie und die Zahlen. Ihr Blick war ruhiger als der ihres Bruders. Manchmal war das hilfreich. Manchmal unbequem.

Der Anwalt hatte die Unterlagen vor sich. Cybervorfall, Maßnahmen-Matrix, Versicherungsantrag, Protokolle, offene Punkte.

„Wir müssen die Haftungsebenen sauber trennen“, sagte er.

Hartmann rieb sich die Stirn.

„Ich dachte, wir sprechen über einen Angriff.“

„Tun wir“, sagte der Anwalt. „Aber ein Angriff ist nur der Anfang der Prüfung.“

Ein Angriff ist nicht immer Ihr Verschulden

Das ist die erste Entlastung.

Ein Unternehmen kann Opfer eines Cyberangriffs werden, ohne dass die Geschäftsleitung persönlich etwas falsch gemacht hat. Absolute Sicherheit gibt es nicht. Auch gut geführte Unternehmen können getroffen werden.

Die entscheidende Frage lautet deshalb nicht: Ist etwas passiert?

Die entscheidende Frage lautet: War das Unternehmen angemessen vorbereitet, hat die Geschäftsleitung ihre Pflichten organisiert und wurde im Vorfall richtig reagiert?

Genau hier wird aus Technik Verantwortung.

Wenn Risiken bekannt waren und ignoriert wurden, wird es kritisch. Wenn Maßnahmen behauptet, aber nicht umgesetzt wurden, wird es kritisch. Wenn Schulungen ausfallen, Wiederherstellung nie getestet wird, Dienstleisterzugänge ungeprüft bleiben und Protokolle fehlen, entsteht ein anderes Bild.

Nicht der Angriff allein entscheidet über Haftung.

Die Vorgeschichte entscheidet mit.

Erste Ebene: Schaden im Unternehmen

Die naheliegenden Kosten sind schnell sichtbar.

Forensik, Wiederherstellung, Produktionsausfall, Mehrarbeit, Kundenkommunikation, Rechtsberatung, Datenschutzprüfung, mögliche Vertragsstrafen, Versicherungsstreit, Reputationsarbeit.

Diese Kosten treffen zunächst das Unternehmen.

Doch in bestimmten Situationen stellt sich die nächste Frage: Hätte die Geschäftsleitung durch bessere Organisation, Überwachung oder Entscheidung einen Teil des Schadens verhindern oder verringern können?

Dann wird Innenhaftung relevant.

Das eigene Unternehmen kann Ansprüche gegen die Geschäftsleitung prüfen. In Familienunternehmen klingt das fremd. Der Geschäftsführer ist oft Gesellschafter, Familienmitglied, Lebenswerkträger. Aber rechtlich kann die Gesellschaft eigene Ansprüche haben. In der Krise oder bei Gesellschafterstreit, Nachfolge, Verkauf oder Insolvenz wird diese Frage sehr real.

Hartmann sah zu seiner Schwester.

| „Du würdest mich verklagen?“

Sie antwortete nicht sofort.

| „Ich will, dass wir gar nicht erst in diese Lage kommen.“

Das war die bessere Antwort.

Zweite Ebene: Aufsicht und Bußgelder

Neben dem Unternehmensschaden stehen regulatorische Risiken. Je nach Fall können Aufsichtsbehörden prüfen, ob Sicherheits-, Datenschutz-, Melde- oder KI-Pflichten verletzt wurden.

Bußgelder sind dabei nur ein Teil der Gefahr. Schon die Untersuchung bindet Zeit, Aufmerksamkeit und Ressourcen. Sie verlangt Nachweise. Sie stellt Fragen, auf die man besser vorbereitet ist.

Was wurde beschlossen?

Welche Maßnahmen wurden umgesetzt?

Wann wurde ein Vorfall erkannt?

Wann wurde gemeldet?

Welche Daten waren betroffen?

Wie wurden Betroffene geschützt?

Wer war verantwortlich?

Ein Unternehmen, das dann erst beginnt, seine Unterlagen zu suchen, verliert Souveränität.

Dritte Ebene: Beirat und Kontrolle

Carola hatte bis dahin ruhig zugehört.

Dann sagte der Anwalt: „Auch der Beirat sollte Cyber regelmäßig behandeln.“

„Wir sind kein Aufsichtsrat“, sagte sie.

„Das mag sein. Aber wer Kontrolle übernimmt, sollte auch kontrollieren können.“

In vielen Familienunternehmen gibt es Beiräte, Gesellschafterausschüsse oder informelle Kontrollgremien. Ihre rechtliche Stellung kann unterschiedlich sein. Aber praktisch haben sie Einfluss. Sie fragen nach Investitionen, Liquidität, Strategie, Nachfolge, Personal, Immobilien, Finanzierung.

Cyber gehört inzwischen dazu.

Nicht, weil der Beirat technische Details kennen muss. Sondern weil Cyber bestandsrelevant sein kann. Ein Beirat, der nie nach digitaler Resilienz, Versicherung, Krisenplan, KI-Nutzung und Nachweisen fragt, übersieht einen wesentlichen Teil moderner Unternehmensrisiken.

Carola schrieb sich drei Punkte auf:

Cyber-Lagebild.

Versicherung.

Krisenübung.

Das war ein Anfang.

Vierte Ebene: Versicherung und Deckung

Hartmann hoffte auf die Versicherung.

Das ist menschlich. Versicherung ist dafür da, Restrisiken tragbar zu machen. Aber Versicherung ersetzt keine Pflichtenerfüllung.

Cyber-Police, D&O und Strafrechtsschutz haben unterschiedliche Funktionen. Die Cyber-Police betrifft in der Regel das Unternehmen und definierte Cyberfolgen. Die D&O betrifft persönliche Haftungsansprüche gegen Organpersonen. Strafrechtsschutz betrifft Verteidigungskosten in bestimmten Verfahren.

Wer diese Verträge erst im Schadensfall auseinanderhält, liest mit hohem Puls.

Noch schwieriger wird es, wenn Antragsangaben und Wirklichkeit auseinanderfallen. Wenn Sicherheitsmaßnahmen im Antrag bejaht wurden, die im Unternehmen nicht durchgängig bestanden, entsteht Deckungsdruck. Wenn Pflichten bewusst ignoriert wurden, können Ausschlüsse relevant werden.

Die beste Versicherung ist nicht die, die man im Schadensfall verzweifelt auslegt.

Die beste Versicherung ist die, deren Voraussetzungen man vorher kennt und erfüllt.

Fünfte Ebene: Verhalten nach dem Vorfall

Der Anwalt wurde an diesem Punkt besonders klar.

„Viele Haftungsrisiken entstehen nicht durch den Angriff, sondern durch das Verhalten danach.“

Zu spätes Melden. Unvollständige Information. Beschwichtigung ohne Grundlage. Vorschnelles Löschen von Beweisen. Widersprüchliche Aussagen gegenüber Kunden, Banken, Versicherern oder Behörden. Einsame Entscheidungen über Lösegeld. Fehlende Einbindung von Datenschutz, Forensik und Rechtsberatung.

In der Krise steht die Geschäftsleitung unter Druck. Genau deshalb müssen die Wege vorher festgelegt werden.

Wer in der Krise improvisiert, trifft nicht automatisch falsche Entscheidungen. Aber er erhöht die Wahrscheinlichkeit.

Haftung liebt schlechte Dokumentation.

Die Verteidigung heißt nicht Perfektion

Hartmann fragte, was ihn wirklich entlasten könne.

Die Antwort war nicht: Perfektion.

Kein Unternehmen wird jede Maßnahme perfekt umsetzen. Kein Geschäftsführer wird jedes Detail kennen. Kein Beirat wird jeden technischen Bericht durchdringen. Perfektion ist kein realistischer Maßstab.

Entlastend ist etwas anderes:

Eine angemessene Organisation.

Informierte Entscheidungen.

Regelmäßige Überwachung.

Dokumentierte Nachweise.

Ehrliche Risikobewertung.

Schnelle und geordnete Reaktion.

Klare Eskalationswege, gezielte Einbindung von Fachleuten.

Wer zeigen kann, dass er diese Punkte ernst genommen hat, steht anders da als jemand, der nur sagt: „Das müsste unsere IT gemacht haben.“

Der Haftungsordner

Frau Weber nannte ihn nicht Haftungsordner. Sie nannte ihn Cockpit-Unterlagen. Das klang besser.

Darin sollten künftig liegen:

Geschäftsleitungsbeschlüsse zu Cyber und KI.

Maßnahmen-Matrix.

Schulungsnachweise.

Berichte der IT.

Nachweise zu Backups und Wiederherstellungstests.

Lieferantenprüfungen.

KI-Inventur.

Versicherungsunterlagen.

Protokolle von Vorfällen und Übungen.

Beiratsberichte.

Hartmann sah die Liste: „Das ist viel Papier.“

„Nein“, sagte Weber. „Das ist unsere Geschichte, falls jemand fragt.“

Genau darum geht es.

Nachweise erzählen die Geschichte der Sorgfalt. Ohne Nachweise erzählen andere die Geschichte für Sie.

MEMO

1. Welche Haftungsebenen kann ein Cybervorfall in Ihrem Unternehmen berühren?
2. Können Sie nachweisen, dass die Geschäftsleitung Cyber-Risiken behandelt hat?
3. Gibt es dokumentierte Entscheidungen zu Maßnahmen sowie Restunsicherheiten und Budgets?
4. Wird der Beirat oder ein Kontrollgremium regelmäßig informiert?
5. Sind Cyber-Police, D&O und Strafrechtsschutz sauber abgegrenzt?
6. Gibt es einen Plan für Verhalten nach dem Vorfall?
7. Wer führt die Nachweisakte?

Hartmann hatte verstanden: Haftung beginnt nicht erst mit dem Anwaltsschreiben.

Sie beginnt mit dem, was vorher unterlassen, entschieden oder dokumentiert wurde.

Und wenn trotzdem der Bildschirm schwarz wird, zählt vor allem eines:

Die Reihenfolge der ersten Stunden.

12 | Wenn es brennt: Die ersten 72 Stunden

05:17 Uhr.

Der Anruf aus der Produktion. Das ERP verschlüsselt. Die Halle kurz vor der Frühschicht. Der Text auf den Bildschirmen. Die Frist. Der Betrag. Die Frage, ob man noch führt oder nur noch reagiert.

Im Prolog haben wir diesen Moment erlebt.

Jetzt nehmen wir ihn wieder auf.

Denn in einer Cyberkrise entscheidet nicht nur, was passiert ist. Es entscheidet, in welcher Reihenfolge gehandelt wird.

Die erste Regel: nicht hektisch retten

Hartmann wollte handeln. Sofort.

Das ist verständlich. Unternehmer sind darauf trainiert, Probleme zu lösen. Maschine steht? Ursache finden. Kunde droht abzuspringen? Anrufen. Bank stellt Fragen? Zahlen liefern. Mitarbeiter braucht Entscheidung? Treffen.

In der Cyberkrise kann dieser Reflex gefährlich werden.

Wer Systeme vorschnell ausschaltet, kann Spuren verlieren. Wer ungeprüft Backups einspielt, kann den Angreifer wieder einladen. Wer Daten löscht, vernichtet Beweise. Wer zu früh kommuniziert, behauptet vielleicht Dinge, die später nicht halten. Wer gar nicht kommuniziert, erzeugt Gerüchte.

Die erste Regel lautet deshalb:

Nicht hektisch retten. Erst ordnen.

Ordnung heißt nicht Untätigkeit. Ordnung heißt kontrolliertes Handeln.

Minute 1 bis 30: isolieren und dokumentieren

IT-Leiter Baumann gab am Telefon die erste Anweisung:

„Betroffene Systeme vom Netz trennen. Nicht neu starten. Nicht löschen.“

Das war keine perfekte Lösung. Es war die richtige Richtung.

In der ersten Phase geht es darum, weiteren Schaden zu begrenzen und gleichzeitig Spuren zu erhalten. Welche Systeme sind betroffen? Welche Bildschirme zeigen was? Welche Uhrzeit? Wer hat was gesehen? Welche Maßnahmen wurden wann ergriffen?

Weber, die kaufmännische Leiterin, begann ein Krisenprotokoll auf Papier.

Nicht im ERP. Nicht in einem geteilten Ordner. Nicht in einem System, das selbst betroffen sein konnte.

Auf Papier.

05:17 Uhr: Anruf Keller.

05:34 Uhr: Hartmann im Werk.

05:41 Uhr: erste Systeme isoliert.

05:50 Uhr: IT-Leiter vor Ort.

06:03 Uhr: Frühschicht informiert.

Ein solches Protokoll wirkt im Moment banal. Später ist es Gold wert. Es hilft Forensik, Versicherung, Rechtsberatung, Behördenkommunikation und interner Aufarbeitung.

Erinnerungen werden in Krisen weich. Protokolle bleiben härter.

Der Krisenstab

Um 06:10 Uhr saßen die richtigen Menschen nicht alle am Tisch. Aber die wichtigsten waren identifiziert.

Geschäftsleitung.

IT.

Produktion.

Kaufmännische Leitung.

Datenschutz.

Kommunikation.

Externe Forensik.

Rechtsberatung.

Versicherung.

Nicht jeder muss ständig im Raum sein. Aber jeder muss erreichbar sein. Und es muss klar sein, wer entscheidet.

Ein Krisenstab ist kein Diskussionsclub. Er ist die Struktur, die verhindert, dass zehn Menschen gleichzeitig gut gemeinte, aber widersprüchliche Entscheidungen treffen.

Hartmann legte fest:

Alle Informationen laufen über Weber und Baumann.

Keine Systeme werden ohne Freigabe gestartet.

Kundenkommunikation erfolgt zentral.

Mitarbeiter erhalten kurze, regelmäßige Informationen.

Externe Kommunikation wird abgestimmt.

Das war noch keine Lösung. Aber es war Führung.

Die erste Mitarbeiterinformation

Die Frühschicht stand in der Halle.

Menschen mit Thermobechern, Sicherheitsschuhen, Jacken. Sie erwarteten Arbeit. Stattdessen sahen sie stehende Maschinen und gespannte Gesichter.

Hartmann trat vor die Mitarbeiter.

Er sagte nicht mehr, als er wusste.

„Wir haben einen Cybervorfall. Die IT arbeitet mit externen Spezialisten. Niemand startet Systeme neu. Niemand steckt Kabel ein. Informationen laufen über die benannten Ansprechpartner. Wir melden uns wieder, sobald wir belastbar mehr sagen können.“

Das war knapp. Aber richtig.

In der Krise ist Kommunikation keine Beruhigungsmassage. Sie ist Orientierung. Wer nichts sagt, überlässt den Raum Gerüchten. Wer zu viel sagt, schafft später Probleme.

Gute Kommunikation unterscheidet zwischen sicherem Wissen, Vermutung und offenem Punkt.

Die Meldeuhren

Am Vormittag kam das Thema Fristen auf.

War ein meldepflichtiger Sicherheitsvorfall gegeben? Waren personenbezogene Daten betroffen? Gab es Hinweise auf Datenabfluss? Welche Behörden, Kunden, Versicherer oder Vertragspartner mussten informiert werden? Welche Fristen?

In Cybervorfällen können mehrere Uhren gleichzeitig laufen.

Eine Uhr für Sicherheitsvorfälle.

Eine Uhr für Datenschutzverletzungen.

Eine Uhr für Versicherungsobliegenheiten.

Eine Uhr für vertragliche Kundenmeldungen.

Eine Uhr für interne Gremien.

Wer nur auf eine Uhr schaut, kann die andere verpassen.

Deshalb gehört die Meldekette nicht erst in die Krise. Sie gehört in den Notfallplan.

Hartmann merkte, dass sie viele Informationen noch nicht hatten. Das ist normal. Meldungen müssen oft mit vorläufigem Kenntnisstand erfolgen und später ergänzt werden. Warten auf vollständige

Gewissheit kann riskanter sein als eine sorgfältig formulierte Erstmeldung.

Melden ist nicht automatisch ein Schuldeingeständnis.

Es ist in vielen Fällen Teil geordneter Führung.

Die Lösegeldfrage

Gegen neun Uhr stellte jemand die Frage, die alle im Raum dachten.

| „Zahlen wir?“

Hartmann schwieg.

Der Betrag auf dem Bildschirm war hoch. Aber der Produktionsausfall war ebenfalls teuer. Kunden warteten. Mitarbeiter standen. Das Unternehmen verlor mit jeder Stunde Geld und Vertrauen.

Gerade deshalb darf diese Entscheidung nicht einsam und nicht im Affekt getroffen werden.

Lösegeldzahlung ist kein normaler Einkauf. Man verhandelt mit Kriminellen. Es gibt keine Garantie, dass Daten entschlüsselt werden. Es gibt keine Garantie, dass abgeflossene Daten nicht doch veröffentlicht werden. Es können rechtliche, sanktionsbezogene, versicherungsrechtliche und strategische Fragen entstehen.

Die wichtigste Antwort auf die Lösegeldfrage wird nicht in der Krise gegeben.

Sie wird vorher gegeben: durch Rechtsprüfung, getestete Backups, Notfallpläne, Forensik-Kontakte, Versicherungsklarheit und Entscheidungswege.

Wenn man sauber wiederherstellen kann, sinkt der Druck. Wenn man es nicht kann, verhandelt man mit schwacher Hand.

Der zweite Schock: Datenabfluss

Am Nachmittag meldete die Forensik einen Verdacht.

Es ging möglicherweise nicht nur um Verschlüsselung. Es konnte auch Datenabfluss gegeben haben.

Damit änderte sich die Lage.

Ein Backup hilft gegen Stillstand. Es hilft nicht gegen Kopien, die bereits draußen sind. Aus einem reinen Verfügbarkeitsproblem wird ein Datenschutz-, Kommunikations- und Vertrauensproblem.

Jetzt musste geprüft werden:

Welche Daten könnten betroffen sein?

Kunden? Lieferanten? Mitarbeiter? Technische Informationen? Finanzdaten?

Besteht ein Risiko für betroffene Personen?

Müssen Kunden informiert werden?

Muss die Datenschutzaufsicht eingebunden werden?

Welche Formulierungen sind belastbar?

Doppelte Erpressung lebt genau von diesem Druck: Lösegeld zahlen, sonst veröffentlichen wir die Daten.

Auch hier gilt: nicht Panik, sondern Ordnung.

Der Wiederanlauf

Die Produktion wollte wieder laufen.

Keller drängte. Verständlicherweise. Jeder Tag Stillstand kostete Geld. Einige Aufträge konnten mit Papier, Erfahrung und telefonischer Abstimmung teilweise bearbeitet werden. Aber das war begrenzt.

Baumann warnte: „Wenn wir zu früh hochfahren, wissen wir nicht, ob der Angreifer noch im System ist.“

Das ist eine der schwersten Entscheidungen in der Krise. Der Betrieb will weiter. Die Forensik will verstehen. Die Geschäftsleitung muss zwischen Ausfallkosten und Wiederinfektionsrisiko abwägen.

Wiederanlauf ist nicht nur Technik. Es ist eine Geschäftsentscheidung unter Unsicherheit.

Deshalb braucht es klare Kriterien:

Welche Systeme sind sauber?

Welche Backups sind vertrauenswürdig?

Welche Zugänge wurden geschlossen?

Welche Mindestprozesse braucht der Betrieb?

Welche Risiken akzeptieren wir vorübergehend?

Wer entscheidet?

Hartmann lernte: Schnell ist nicht immer schnell. Ein zu früher Wiederanlauf kann die Krise verlängern.

Nach 72 Stunden

Drei Tage später war die Krise nicht vorbei.

Aber sie war geordnet.

Die wichtigsten Systeme waren priorisiert. Die Kommunikation lief zentral. Die Meldungen waren auf den Weg gebracht oder vorbereitet. Die Forensik hatte erste Erkenntnisse. Kunden erhielten eine sachliche Information. Mitarbeiter wussten, wo sie Fragen stellen konnten. Die Versicherung war eingebunden. Der Beirat informiert.

Hartmann hatte nicht alles richtig gemacht. Aber er hatte geführt.

Der Unterschied war sichtbar.

Ein Unternehmen ohne Plan hätte in diesen 72 Stunden hektisch reagiert, widersprüchlich kommuniziert und Beweise gefährdet. Hartmann Maschinenbau hatte immer noch Schaden. Aber es hatte eine nachvollziehbare Geschichte.

MEMO

1. Gibt es einen Notfallplan, der auch ohne IT erreichbar ist?
2. Ist geregelt, wer in der ersten Stunde entscheidet?
3. Wissen Mitarbeiter, was sie nicht tun dürfen?
4. Gibt es externe Forensik- und Rechtskontakte vor dem Vorfall?
5. Sind Meldepflichten und Versicherungsobliegenheiten in einer Meldekette abgebildet?
6. Gibt es vorbereitete Kommunikationslinien für Mitarbeiter und Kunden?
7. Wurde der Wiederanlauf schon einmal geübt?

Hartmann schrieb später einen Satz auf die erste Seite seines Notfallplans:

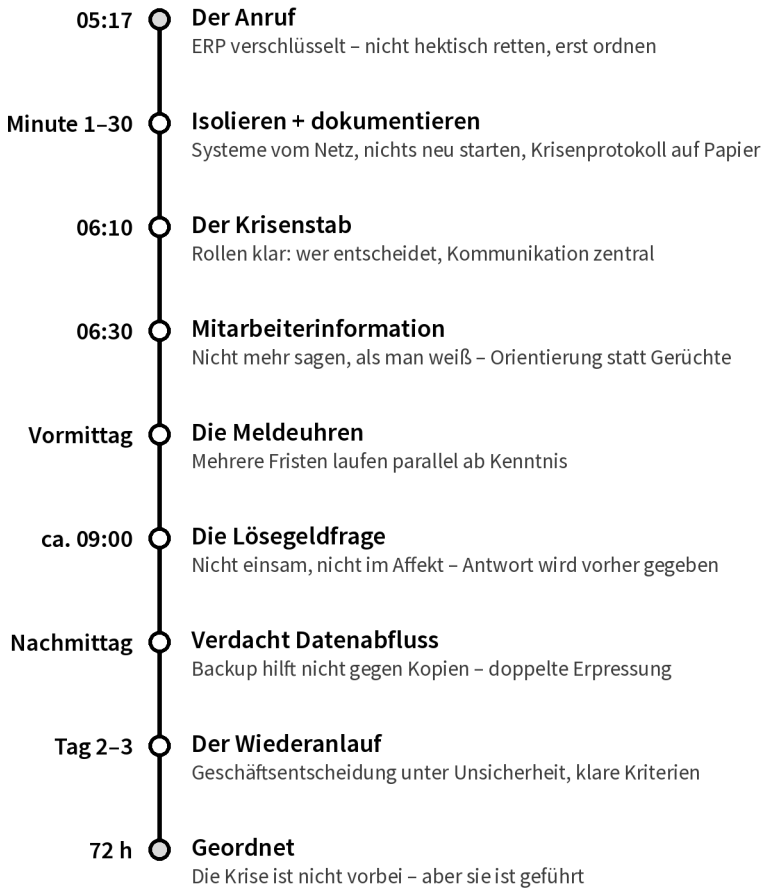
| „In der Krise zählt Reihenfolge.“

Mehr musste dort nicht stehen.

Denn wer die Reihenfolge nicht kennt, verliert Zeit, Beweise und Vertrauen.

Die ersten 72 Stunden

Reihenfolge statt Hektik



„In der Krise zählt Reihenfolge.“

Nach den ersten 72 Stunden kam die nächste Ernüchterung.

Die Police lag auf dem Tisch. Aber gekauft war noch lange nicht gedeckt.

13 | Gekauft ist nicht gedeckt

Der Brief des Versicherers war höflich.

Das machte ihn nicht angenehmer.

Zehn Tage nach dem Vorfall lief die Produktion bei Hartmann Maschinenbau wieder, aber noch nicht normal. Die Forensiker hatten erste Berichte geliefert. Weber hatte Kosten gesammelt. Mehrarbeit, Ausfall, Dienstleister, Kommunikation, Rechtsberatung, Wiederherstellung.

Unten stand eine Zahl, die niemand gern ansah.

Hartmann war trotzdem nicht verzweifelt. Er hatte eine Cyber-Police. Ordentlich abgeschlossen. Prämie bezahlt. Ansprechpartner bekannt. Police im Ordner.

Dann kam der Brief.

Der Versicherer prüfe die Eintrittspflicht. Bestimmte Angaben aus dem Antrag seien mit der tatsächlichen Sicherheitslage abzugleichen. Es gebe Rückfragen zu Mehr-Faktor-Authentifizierung, Backup-Tests, Patch-Management, Fernwartungszugängen und Meldung.

Hartmann las den Brief zweimal.

Beim zweiten Mal wurde er nicht ruhiger.

Eine Police ist kein Freibrief

Viele Unternehmer behandeln Versicherungen wie eine Beruhigungsspielle.

Abgeschlossen. Beahlt. Erledigt.

Im Cyberbereich ist das gefährlich.

Eine Versicherung übernimmt nicht jede denkbare digitale Krise. Sie leistet im Rahmen eines Vertrags. Dieser Vertrag enthält Bedingungen, Obliegenheiten, Ausschlüsse, Sublimits, Meldefristen, Sicherheitsanforderungen und Definitionen.

Das ist nicht böse. Das ist Versicherung.

Der Versicherer übernimmt ein Risiko auf Grundlage bestimmter Angaben. Wenn diese Angaben ungenau, zu optimistisch oder veraltet sind, entsteht im Schadensfall Streit.

Hartmann hatte beim Abschluss nicht bewusst falsche Angaben gemacht. Er hatte geantwortet, wie viele Unternehmer antworten: nach bestem Gefühl, gestützt auf IT-Aussagen, in der Annahme, dass es schon passen werde.

Aber Gefühl ist kein Nachweis.

Antrag gegen Wirklichkeit

Frau Weber legte den Versicherungsantrag neben die Maßnahmen-Matrix.

Mehr-Faktor-Authentifizierung für externe Zugänge?

Im Antrag: ja.

In der Wirklichkeit: weitgehend, aber nicht überall. Der alte Fernwartungszugang war unklar.

Regelmäßige Backups?

Im Antrag: ja.

In der Wirklichkeit: Sicherungen liefen, aber der Wiederherstellungstest war zuletzt abgebrochen und nicht nachgeholt worden.

Patch-Management?

Im Antrag: ja.

In der Wirklichkeit: für viele Systeme strukturiert, für einige produktionsnahe Systeme mit Ausnahmen.

Schulungen?

Im Antrag: ja.

In der Wirklichkeit: einzelne Schulungen, aber kein klarer Rhythmus und keine vollständige Dokumentation.

Die Liste war nicht katastrophal. Aber sie war nicht deckungsgleich.

Der Antrag beschrieb das Unternehmen, wie es sein sollte. Die Wirklichkeit zeigte das Unternehmen, wie es war.

Dazwischen entstand Risiko.

Cyber-Police, D&O und Strafrechtsschutz

Hartmann sprach von „der Versicherung“.

Der Anwalt korrigierte ihn.

| „Welche?“

Das war keine Spitzfindigkeit.

Eine Cyber-Police kann Eigenschäden des Unternehmens abdecken: Forensik, Wiederherstellung, Betriebsunterbrechung, Krisenkommunikation, bestimmte Haftpflichtansprüche.

Eine D&O-Versicherung betrifft persönliche Vermögensschäden von Organpersonen, wenn ihnen Pflichtverletzungen vorgeworfen werden.

Ein Strafrechtsschutz kann Verteidigungskosten in Ermittlungsverfahren abdecken.

Drei Verträge. Drei Funktionen. Drei Prüfungen.

Wer sie erst im Schadensfall auseinanderhält, verliert Zeit.

Hartmann erkannte, dass die Versicherungsakte nicht nur Sache der kaufmännischen Leiterin war. Sie gehörte auch ins Cockpit der Geschäftsleitung.

Obliegenheiten müssen in den Notfallplan

Versicherungsverträge enthalten Pflichten im Schadensfall.

Wann muss gemeldet werden?

Welche Dienstleister dürfen beauftragt werden?

Muss der Versicherer vor bestimmten Maßnahmen zustimmen?

Welche Informationen sind zu liefern?

Was darf nicht verändert werden?

Welche Kosten sind freigabepflichtig?

Diese Fragen gehören nicht in einen Ordner, den man erst öffnet, wenn die Halle steht. Sie gehören in den Notfallplan.

Frau Weber ergänzte deshalb die Krisencheckliste:

Versicherer informieren.

Policennummer und Hotline.

Obliegenheiten prüfen.

Freigaben dokumentieren.

Kommunikation mit Anwalt abstimmen.

Kosten separat erfassen.

Das war kein Misstrauen gegenüber dem Versicherer. Es war Professionalität.

CEO-Fraud ist nicht automatisch Cyberdeckung

Der Fall der Buchhalterin Frau Berger zeigte eine weitere Lücke.

Die vierundachtzigtausend Euro waren durch Manipulation entstanden. Eine E-Mail, angeblich von Hartmann, eine geänderte Bankverbindung, eine reguläre Überweisung.

| „Das ist doch Cyber“, sagte jemand.

Vielleicht. Vielleicht nicht.

Ob ein solcher Schaden gedeckt ist, hängt vom konkreten Vertrag ab. Manche Policen decken bestimmte Formen von Social Engineering oder Zahlungsbetrug. Andere nur mit Zusatzbausteinen. Manche schließen solche Fälle aus oder begrenzen sie stark.

Für die Geschäftsleitung folgt daraus:

Nicht Begriffe entscheiden, sondern Bedingungen.

| „Cyber“ ist kein Zauberwort.

Eine digitale Täuschung kann versicherungsrechtlich anders behandelt werden als eine technische Kompromittierung. Deshalb müssen typische Szenarien vorab gegen die Police gespiegelt werden.

Ausschlüsse und harte Ränder

Versicherungen haben Ränder.

Bekannte, aber niemals behobene Schwachstellen. Unzutreffende Antragsangaben. Verspätete Meldung. Bestimmte Kriegs- oder Hoheitsrisiken. Nicht autorisierte Kosten. Fehlende Sicherheitsmaßnahmen. Vorsätzliche Pflichtverletzungen.

Nicht jeder Ausschluss greift leicht. Nicht jeder Versicherer wird sich entziehen. Aber die Geschäftsleitung sollte die Ränder kennen.

Wer seine Police nur als Deckungssumme liest, versteht sie nicht.

Wichtiger als die Summe ist oft die Frage:

Wann zahlt sie?

Wann nicht?

Was müssen wir tun, damit sie zahlt?

Die Versicherung als Hausaufgabenliste

Nach dem ersten Ärger nutzte Hartmann den Versicherungsantrag anders.

Nicht mehr nur als Vertragsdokument.

Als Hausaufgabenliste.

Wenn der Versicherer nach Mehr-Faktor-Authentifizierung fragt, ist das nicht nur eine Bedingung. Es ist ein Hinweis auf eine wichtige Maßnahme.

Wenn er nach Backups und Wiederherstellung fragt, zeigt er ein zentrales Risiko.

Wenn er Schulungen, Patch-Management und Fernzugänge anspricht, benennt er typische Schadenursachen.

Damit kann die Police helfen, Sicherheit zu strukturieren. Aber nur, wenn man Antrag und Wirklichkeit regelmäßig abgleicht.

Frau Weber schlug einen jährlichen Versicherungsabgleich vor:

Was steht im Antrag?

Was hat sich im Unternehmen verändert?

Welche Maßnahmen sind weggefallen oder hinzugekommen?

Welche Angaben müssen aktualisiert werden?

Welche neuen Szenarien sollten versichert werden?

Welche Obliegenheiten gehören in den Notfallplan?

Das war vernünftig.

Versicherung ist kein Dokument für den Schrank. Sie ist Teil der Risikosteuerung.

MEMO

1. Kennen Sie den genauen Deckungsumfang Ihrer Cyber-Police?
2. Sind Cyber-Police, D&O und Strafrechtsschutz sauber abgegrenzt?
3. Stimmen Antragsangaben und Wirklichkeit überein?
4. Sind Versicherungsobliegenheiten im Notfallplan abgebildet?
5. Sind typische Szenarien wie Ransomware, Datenabfluss, Betriebsunterbrechung, Dienstleistervorfall und CEO-Fraud geprüft?
6. Gibt es jährliche Abstimmung zwischen Geschäftsleitung, IT, Versicherungsmakler und Rechtsberatung?
7. Können Sie Sicherheitsmaßnahmen belegen, die im Antrag vorausgesetzt wurden?

Hartmann legte den Versicherungsbrief in den Cockpit-Ordner.

Nicht zu den schlechten Nachrichten.

Zu den Lehrmitteln.

Denn manche Dokumente zahlen nicht sofort.

Aber sie zeigen sehr genau, wo ein Unternehmen seine Nahtstellen prüfen muss.

Und damit war Hartmann bereit für das wichtigste Instrument der nächsten Monate:

Das Cockpit.

Teil V – Die Ordnung

Wie aus dem Weckruf eine Führungsroutine entsteht

14 | Das Cockpit: Nachweis statt Nervosität

Der Brief der Aufsicht kam ohne Drama.

Kein Blaulicht. Keine Schlagzeile. Kein Anruf um 05:17 Uhr.

Nur ein höfliches Schreiben mit Frist.

Man bitte um Darlegung, welche Maßnahmen zur Informationssicherheit getroffen, wie deren Umsetzung überwacht und welche Nachweise hierzu geführt würden.

Hartmann las den Brief.

| „Wir machen doch einiges“, sagte er.

Herr Baumann nickte.

| „Ja. Aber nicht alles ist sauber dokumentiert.“

Frau Weber sagte nichts. Sie ging zum Schrank und holte den roten Ordner.

Das war der Moment, in dem Hartmann verstand:

Tun ist die halbe Miete. Beweisen ist die andere Hälfte.

Kein Berichtswesen für Bürokraten

Viele Unternehmer reagieren allergisch auf zusätzliche Dokumentation.

Noch ein Ordner. Noch eine Liste. Noch ein Protokoll. Noch ein Nachweis. Noch eine Ampel.

Diese Skepsis ist verständlich. Schlechte Dokumentation kostet Zeit und schafft keine Sicherheit. Sie dient nur dazu, Häkchen zu produzieren.

Ein gutes Cockpit ist anders.

Es zeigt der Geschäftsleitung, wo das Unternehmen steht, welche Risiken offen sind, welche Maßnahmen wirken, wo Entscheidungen fehlen und welche Nachweise existieren.

Es ist kein Archiv. Es ist ein Führungsinstrument.

Hartmann brauchte kein Reporting-Monster. Er brauchte eine Übersicht, die Entscheidungen ermöglicht.

Sechs Instrumente

Weber schrieb sechs Instrumente an das Whiteboard.

Erstens: Geschäftsleitungsprotokoll.

Wann wurde Cyber behandelt? Welche Entscheidungen wurden getroffen? Welche Risiken wurden akzeptiert? Welche Maßnahmen wurden beauftragt? Wer ist verantwortlich?

Zweitens: Maßnahmen-Matrix.

Die zehn Führungsfragen aus Kapitel 7 mit Status, Nachweis, Verantwortlichem, Termin und Entscheidung.

Drittens: Schulungsnachweis.

Wer wurde geschult? Wann? Zu welchem Inhalt? Auch Geschäftsleitung, Beirat und neue Mitarbeiter.

Viertens: Incident-Log.

Nicht nur Großvorfälle. Auch kleinere Ereignisse, Verdachtsfälle, Simulationen, Erkenntnisse und Nachbesserungen.

Fünftens: Lieferantenakte.

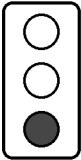
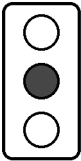
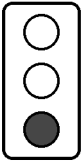
Kritische Dienstleister, Zugänge, Verträge, Nachweise, Meldewege, Prüfdatum.

Sechstens: KI-Inventur.

Welche KI-Werkzeuge, welche Zwecke, welche Daten, welche Freigaben, welche Prüfregeln.

Mehr brauchte es für den Anfang nicht.

Weniger wäre zu wenig gewesen.

Cockpit		
Schulungsquote: 92 % fehlende Schulungen terminiert		grün
MFA-Quote: 78 % Zugänge Home-Office klären		gelb
Incident-Log: kleinere Vorfälle abgewehrt		grün
Ampelregel: Unklar ist nicht grün.		

Die Ampel muss ehrlich sein

Baumann schlug eine Ampel vor.

Grün, gelb, rot.

Hartmann war skeptisch. Ampeln können beruhigen, wenn sie ehrlich sind. Sie können gefährlich werden, wenn sie geschönt sind.

Frau Weber legte deshalb eine Regel fest:

Unklar ist nicht grün.

Unklar ist gelb oder rot, bis es belegt ist.

Das war entscheidend.

Viele Unternehmen erklären Punkte für erledigt, weil jemand glaubt, dass sie erledigt sind. „Backup läuft.“ „Dienstleister ist sicher.“ „Mitarbeiter sind geschult.“ „KI nutzen wir kaum.“ „Versicherung passt.“

Ein Cockpit fragt nicht nach Gefühl.

Es fragt nach Nachweis.

Wann wurde der Wiederherstellungstest durchgeführt?

Wo liegt das Protokoll?

Welche Mitarbeiter haben teilgenommen?

Welche Dienstleister haben kritischen Zugriff?

Welche KI-Tools wurden freigegeben?

Welche Protokolle belegen die Geschäftsleitungsentscheidung?

Erst dann wird aus Behauptung Steuerung.

Kennzahlen, die eine Geschäftsleitung versteht

Hartmann wollte keine technischen Detailtabellen.

| „Ich brauche fünf Zahlen, die mir etwas sagen“, sagte er.

Baumann und Weber einigten sich auf einen ersten Satz:

- Anteil kritischer Zugänge mit Mehr-Faktor-Schutz
- Datum des letzten erfolgreichen Wiederherstellungstests
- Anzahl offener kritischer Schwachstellen älter als definierte Frist
- Anteil geschulter Mitarbeiter und Führungskräfte
- Anteil geprüfter kritischer Dienstleister
- Anzahl freigegebener und nicht freigegebener KI-Werkzeuge

Das waren sechs, nicht fünf. Hartmann akzeptierte es.

Die Zahlen mussten nicht perfekt sein. Sie mussten ehrlich und wiederkehrend sein.

Einmalige Zahlen sind Momentaufnahmen. Wiederkehrende Zahlen zeigen Entwicklung.

Das offene Ticket

Beim Aufbau des Cockpits fand Baumann ein altes Ticket.

Restore-Test abgebrochen. Wiederholung erforderlich.

Status: offen.

Datum: vor sieben Monaten.

Niemand hatte es böse liegen lassen. Es war im Alltag verschwunden. Kunden, Maschinen, Urlaube, Projekte, andere Prioritäten. Ein offenes Ticket unter vielen.

Hartmann las den Satz:

| „Wiederholung erforderlich.“

Mehr stand dort nicht.

Aber es reichte.

Ein offenes Ticket ist kein erledigtes Risiko. Es ist ein Risiko mit Aktenzeichen.

Das Cockpit holte diesen Punkt nach oben. Nicht, weil die IT schlecht gearbeitet hatte. Sondern weil es ein System brauchte, das offene Risiken sichtbar hält, bis sie entschieden oder gelöst sind.

Nachweis ist Substanz

Hartmann begann, Dokumentation anders zu sehen.

Nicht mehr als Papier für Dritte. Sondern als Teil der Unternehmenssubstanz.

Ein Unternehmen, das verkaufen, finanzieren, versichern, übergeben oder in große Lieferketten eingebunden werden will, muss Vertrauen zeigen können. Vertrauen entsteht nicht nur durch Namen, Geschichte und Qualität. Es entsteht zunehmend durch Nachweise.

Kann das Unternehmen mit Vorfällen umgehen?

Sind Daten geschützt?

Ist KI geregelt?

Sind Dienstleister geprüft?

Sind Führung und Beirat eingebunden?

Sind Versicherungen belastbar?

Ein gutes Cockpit beantwortet diese Fragen nicht nur im Krisenfall.
Es beantwortet sie im Alltag.

Der Rhythmus

Frau Weber schlug einen festen Rhythmus vor.

Monatlich: operative IT- und Maßnahmenprüfung.

Quartalsweise: Cockpit-Bericht an die Geschäftsleitung.

Halbjährlich: Bericht an Beirat oder Gesellschafterkreis.

Jährlich: Review von Versicherung, Lieferanten, KI-Inventur, Notfallübung und Betroffenheitsprüfung.

Hartmann fand das zunächst viel.

Dann verglich er es mit anderen Routinen: Monatsabschluss, Liquiditätsplanung, Qualitätsmanagement, Arbeitssicherheit, Steuerfristen, Bankreporting.

Unternehmen leben von wiederkehrender Ordnung.

Cyber muss Teil dieser Ordnung werden.

Die Antwort an die Aufsicht

Als Hartmann die Antwort vorbereiten ließ, war sie nicht perfekt.

Aber sie war belastbar.

Sie enthielt die Maßnahmen-Matrix. Protokolle. Schulungsplan. Restore-Test-Termin. Lieferantenübersicht. KI-Inventur. Versicherungsabgleich. Offene Punkte mit Fristen.

Das war wichtig: Auch offene Punkte durften genannt werden, wenn sie eingeordnet und bearbeitet waren.

Ein Unternehmen muss nicht behaupten, fertig zu sein. Es muss zeigen, dass es führt.

Memo für die Geschäftsleitung

1. Gibt es ein Cockpit, das Geschäftsleitung und Beirat verstehen?
2. Welche Nachweise liegen tatsächlich vor?
3. Welche Punkte wurden nur behauptet?
4. Gibt es ehrliche Ampellogik?
5. Welche Kennzahlen zeigen Entwicklung statt Momentaufnahme?
6. Wie oft wird berichtet?
7. Wer ist Eigentümer des Cockpits?

Hartmann legte den Brief der Aufsicht in die Akte.

Zum ersten Mal empfand er die Frist nicht nur als Druck.

Sie zwang ihn, sichtbar zu machen, was im Unternehmen zu lange verteilt gewesen war.

Und als das Cockpit stand, stellte seine Schwester Carola die nächste Frage:

„Warum sehe ich das eigentlich erst jetzt?“

Damit war der Beirat im Spiel.

15 | Der Beirat auf dem Wachturm

Carola Hartmann war nicht leicht zu beeindrucken.

Sie hatte das Unternehmen nicht operativ geführt, aber sie kannte Familienunternehmen. Sie wusste, dass Zahlen nicht die ganze Wahrheit erzählen. Sie wusste auch, dass ein ruhiger Geschäftsführer nicht immer bedeutet, dass ein Risiko unter Kontrolle ist.

Im nächsten Beirat legte Thomas Hartmann das Cyber-Cockpit vor.

Carola blätterte durch die Unterlagen, sah die Ampeln, die Maßnahmen, die offenen Punkte, den Versicherungsabgleich und die KI-Inventur.

Dann stellte sie die Frage, die im Raum blieb:

„Warum war das bisher kein fester Beiratspunkt?“

Niemand antwortete sofort.

Manchmal sind gute Fragen deshalb gut, weil sie keine lange Einleitung brauchen.

Kontrolle braucht ein Lagebild

Beiräte, Aufsichtsräte, Gesellschafterausschüsse und Familiengremien haben unterschiedliche rechtliche Funktionen. Manche kontrollieren formal, manche beraten, manche strukturieren Familieninteressen, manche haben echte Zustimmungsvorbehalte.

Aber in der Praxis gilt: Wer über Strategie, Investitionen, Risiken und Nachfolge spricht, kann Cyber nicht ausklammern.

Cyber betrifft nicht nur die IT-Abteilung. Cyber betrifft die Fähigkeit, ein Unternehmen fortzuführen. Es betrifft Wert, Reputation, Kundenbeziehungen, Versicherung, Haftung, Finanzierung und Übergabe an die nächste Generation.

Ein Beirat, der regelmäßig über Liquidität, Personal, Markt, Investitionen und Steuern spricht, aber nie über digitale Resilienz, sieht einen Teil des Unternehmens nicht.

Carola formulierte es trocken:

„Wir haben über die neue Halle länger gesprochen als über das System, ohne das in der Halle niemand weiß, was gefertigt werden soll.“

Das stimmte.

Der Beirat muss nicht technisch werden

Hartmann hatte Sorge, dass Cyber den Beirat überfordern würde.

„Die meisten können mit technischen Details nichts anfangen.“

„Dann liefern wir keine technischen Details“, sagte Weber. „Wir liefern Führungsfragen.“

Das ist der richtige Ansatz.

Ein Beirat muss nicht wissen, welche Firewall-Version läuft. Er muss wissen, ob kritische Systeme geschützt, Backups getestet, Dienstleister geprüft, Vorfälle geübt, Versicherungen abgestimmt und KI-Nutzung geregelt sind.

Er muss fragen können:

Was sind die größten offenen Risiken?

Welche Entscheidungen braucht die Geschäftsleitung?

Welche Maßnahmen wurden verschoben und warum?

Welche Vorfälle oder Beinahe-Vorfälle gab es?

Wie belastbar ist die Versicherung?

Wann wurde der Krisenstab zuletzt geübt?

Wie wird die nächste Generation eingebunden?

Das sind keine IT-Fragen. Das sind Kontrollfragen.

Familienunternehmen und blinde Loyalität

In Familienunternehmen kommt eine Besonderheit hinzu.

Vertrauen ist stark. Das ist gut. Es kann aber blind machen.

Man vertraut dem Geschäftsführer oder der Geschäftsführerin, weil es der Bruder, die Cousine, der Vater, die Tochter oder die langjährige Weggefährtin ist. Man vertraut dem IT-Leiter, weil er seit Jahren im Haus ist. Man vertraut der kaufmännischen Leiterin, weil sie alles zusammenhält. Man vertraut der eigenen Unternehmenskultur.

Vertrauen ist wertvoll. Aber Kontrolle ist kein Misstrauen.

Gute Kontrolle schützt Vertrauen.

Carola wollte ihren Bruder nicht kontrollieren, um ihn zu schwächen. Sie wollte verhindern, dass er allein auf einem Risiko sitzt, das die Familie später überrascht.

Das ist die richtige Haltung für Beiräte in Unternehmerfamilien.

Cyber und Nachfolge

Ein Familienunternehmen übergibt heute nicht nur Maschinen, Immobilien, Kundenlisten und Bankbeziehungen.

Es übergibt ein digitales Nervensystem.

ERP, Datenräume, Cloud-Verträge, Zugriffsrechte, KI-Werkzeuge, Kundenportale, Mitarbeiterdaten, Lieferantenzugänge, Backups, Versicherungen, Notfallpläne.

Wenn diese Dinge ungeordnet sind, erbt die nächste Generation nicht nur Vermögen. Sie erbt Risiken.

Carola brachte diesen Punkt in den Beirat ein.

„Wir sprechen seit Jahren über Nachfolge. Aber wir haben noch nie geprüft, ob unsere digitale Ordnung übergabefähig ist.“

Das ist ein starker Satz.

Nachfolgefähigkeit bedeutet heute auch digitale Übergabefähigkeit.

Kann ein neuer Geschäftsführer verstehen, welche Systeme kritisch sind?

Sind Zugänge dokumentiert?

Sind Verträge auffindbar?

Sind Dienstleister bekannt?

Sind Risiken bewertet?

Gibt es ein Cockpit?

Oder hängt alles an drei Köpfen, zwei Excel-Dateien und einem Passworttresor, den nur IT-Leiter Baumann versteht?

Der Beiratsbericht

Weber entwickelte ein schlankes Format für den Beirat.

Eine Seite Überblick.

Drei größte Risiken.

Drei wichtigste Fortschritte.

Drei Entscheidungen oder Eskalationen.

Ampel der Kernbereiche.

Nächste Übung.

Offene Versicherungs- oder Vertragsfragen.

KI-Inventur-Status.

Mehr brauchte der Beirat nicht jedes Mal. Wenn Detailfragen kamen, konnten Anlagen bereitgestellt werden. Aber das Grundformat blieb einfach.

Ein guter Beiratsbericht muss nicht alles zeigen.

Er muss das Richtige sichtbar machen.

Zustimmungsvorbehalte und Budget

Der Beirat hatte in Hartmanns Gruppe Zustimmungsvorbehalte für größere Investitionen.

Bisher waren Cyber-Maßnahmen oft in IT-Budgets versteckt. Ein Teil hier, ein Dienstleister dort, eine Lizenz, ein Projekt. Der Beirat sah Gesamtkosten selten als strategisches Risikobudget.

Das änderte sich.

Cyber-Ausgaben wurden künftig nicht nur als IT-Kosten dargestellt, sondern als Resilienzbudget. Dazu gehörten Technik, Schulung, Forensik-Retainer, Versicherungsprüfung, Notfallübung, KI-Governance und externe Beratung.

Carola fragte nicht: „Warum kostet das so viel?“

Sie fragte: „Welches Risiko reduzieren wir damit?“

Das ist die richtige Budgetfrage.

Der Wachturm

Carola mochte große Bilder nicht. Aber eines akzeptierte sie.

Der Beirat steht nicht im Maschinenraum. Er steht auch nicht am Steuer. Aber er steht hoch genug, um zu fragen, ob der Kurs stimmt und ob Nebel aufzieht.

Dafür braucht er Sicht.

Ein Beirat ohne Lagebild kann nur vertrauen. Ein Beirat mit Lagebild kann Vertrauen durch gute Fragen stärken.

MEMO

1. Wird Cyber regelmäßig im Beirat oder Kontrollgremium behandelt?
2. Erhält das Gremium ein verständliches Lagebild statt technischer Detailberichte?
3. Sind Cyber, KI und Datenschutz Teil der Nachfolgeplanung?
4. Gibt es klare Berichte zu Risiken, Fortschritten und Entscheidungen?
5. Werden Cyber-Ausgaben als Resilienzbudget verstanden?
6. Sind Versicherungs- und Haftungsfragen im Beirat bekannt?
7. Gibt es eine jährliche Krisenübung mit Bericht an das Gremium?

Am Ende der Sitzung sagte Carola:

„Ich will dieses Cockpit jedes Quartal sehen. Nicht, weil ich euch misstraue. Sondern weil ich dem Thema nicht mehr blind vertrauen will.“

Hartmann nickte.

Vor einigen Monaten hätte ihn dieser Satz gestört.

Jetzt war er erleichtert.

Denn Verantwortung, die geteilt sichtbar wird, wiegt weniger als Verantwortung, die allein im Kopf bleibt.

Und nachdem die Gruppe ihre Gremien eingebunden hatte, kamen die Sonderfälle auf den Tisch.

Holding. Ausland. Krise. Finanzkunden. Kritische Infrastruktur.

Hartmann ahnte bereits: Einfacher würde es nicht.

16 | Sonderfälle sind selten Auswege

„Bei uns ist die Lage besonders.“

Diesen Satz hört man in fast jedem Unternehmen.

Manchmal stimmt er. Meistens sogar. Jedes Unternehmen hat Besonderheiten: Gruppenstruktur, Auslandsgesellschaften, Familienholding, Immobiliengesellschaft, Finanzkunden, alte Systeme, spezielle Maschinen, Krise, Wachstum, Nachfolge, einzelne Schlüsselpersonen.

Der Fehler liegt nicht darin, die Besonderheit zu sehen.

Der Fehler liegt darin, aus Besonderheit automatisch Entlastung abzuleiten.

Besonders heißt selten einfacher.

Besonders heißt meistens: genauer prüfen.

Die Holding mit drei Leuten

Hartmanns Cousin führte die Familienholding.

Drei Mitarbeiter. Kein operativer Produktionsbetrieb. Keine Halle. Keine Maschinen. Auf den ersten Blick also weit weg vom Cyber-Thema.

Dann fragte Baumann:

„Wer hält den Gruppenvertrag für das ERP?“

Die Holding.

„Wer verwaltet die zentralen Administratorrechte?“

Formal der Dienstleister, beauftragt über die Holding.

„Wer hält die Versicherungsverträge?“

Die Holding.

„Wer hat Zugriff auf den Datenraum für Beirat und Finanzierung?“

Ebenfalls die Holding.

Drei Mitarbeiter. Aber Schlüssel zu vielen Türen.

Das ist ein typisches Muster.

Kleine Einheiten können große Bedeutung haben, wenn sie zentrale Funktionen, Zugänge oder Verträge halten. Deshalb darf man Gruppen nicht nur nach Kopfzahl betrachten. Man muss nach Rollen fragen.

Jede Gesellschaft, aber nicht isoliert

In Unternehmensgruppen muss jede Gesellschaft betrachtet werden. Tätigkeit, Größe, Rolle, Systeme, Daten, Kunden, Dienstleister.

Aber sie darf nicht isoliert betrachtet werden.

Denn Risiken laufen über Grenzen hinweg. Eine Servicegesellschaft kann IT bereitstellen. Eine Holding kann Verträge halten. Eine Tochter kann Kundendaten verarbeiten. Eine Immobiliengesellschaft kann scheinbar passiv sein, aber zentrale Dokumentenräume nutzen. Eine Auslandsgesellschaft kann andere rechtliche Anforderungen auslösen.

Hartmann ließ ein Gruppenbild erstellen:

Gesellschaften.

Funktionen.

Systeme.

Datenflüsse.

Zugriffsrechte.

Dienstleister.

Kundenanforderungen.

Das Organigramm sah danach weniger schön aus. Aber es war wahrer.

Die Krise als Verstärker

Der nächste Sonderfall war wirtschaftliche Anspannung.

Ein Unternehmen, das gesund ist, kann einen Cybervorfall vielleicht verkraften. Nicht leicht, aber mit Reserven. Ein Unternehmen in Liquiditätsdruck, Sanierung, Nachfolgekonflikt oder Finanzierungsgesprächen kann durch denselben Vorfall in eine gefährliche Lage geraten.

Cyber ist dann nicht nur IT-Risiko. Es ist Krisenverstärker.

Wenn die Produktion steht, kommen weniger Rechnungen raus.

Wenn Kunden abspringen, sinkt Liquidität.

Wenn Forensik und Wiederherstellung teuer werden, steigt Druck.

Wenn Banken gleichzeitig Informationen verlangen, wird Kommunikation kritisch.

Wenn Lösegeld diskutiert wird, entstehen zusätzliche rechtliche und finanzielle Fragen.

Deshalb gehört Cyber in die Krisenfrüherkennung.

Nicht erst, wenn die Krise da ist. Gerade vorher.

Finanzkunden und DORA-Druck

Hartmann Maschinenbau belieferte auch Kunden aus regulierten Branchen. Einer davon war ein Finanzdienstleister, der bestimmte technische Komponenten für interne Prozesse benötigte.

Plötzlich kamen strengere Vertragsklauseln, Audit-Rechte, Meldepflichten und Anforderungen an Dienstleistersteuerung.

„Aber DORA betrifft doch Finanzunternehmen“, sagte Hartmann.

„Direkt vielleicht“, sagte Weber. „Vertraglich kann es trotzdem bei uns ankommen.“

Das ist ein wichtiges Prinzip.

Regulierung wandert über Verträge.

Ein Unternehmen muss nicht selbst Bank oder Versicherer sein, um Anforderungen aus der Finanzwelt zu spüren. Wenn es für regulierte Kunden relevant ist, können deren Pflichten in Einkaufsbedingungen, Sicherheitsanhängen, Audits und Meldewegen weitergereicht werden.

Wieder zeigt sich: Nicht nur unmittelbare Gesetzespflichten zählen. Marktpflichten zählen ebenfalls.

KRITIS und kritische Kunden

Ähnlich ist es bei kritischer Infrastruktur.

Ein Maschinenbauer ist nicht automatisch kritische Infrastruktur. Aber wenn er Komponenten, Wartung oder Dienstleistungen für Energie, Wasser, Gesundheit, Ernährung, Transport oder digitale Infrastruktur liefert, können Anforderungen mittelbar entstehen.

Der Kunde wird fragen:

Wie sichern Sie Lieferfähigkeit?

Wie gehen Sie mit Vorfällen um?

Welche Dienstleister sind beteiligt?

Wie schnell informieren Sie uns?

Welche Wiederanlaufzeiten haben Sie?

Kritische Kunden prüfen ihre Lieferanten nicht aus Neugier. Sie prüfen, weil ihr eigener Ausfall größere Folgen hätte.

Hartmann erkannte: Je wichtiger der Kunde, desto wichtiger die eigene Nachweisfähigkeit.

Ausland ist keine Abkürzung

Die Familiengruppe hatte auch internationale Bezüge. Vertrieb im Ausland, Kunden in mehreren Ländern, Datenübermittlung, externe Dienstleister, Cloud-Anbieter.

Manche Unternehmer hoffen, internationale Struktur mache Pflichten weicher. Oft macht sie sie komplexer.

Andere Aufsichten, andere Kundenanforderungen, Datenschutz bei Drittlandbezug, unterschiedliche Umsetzungen, zusätzliche Verträge, Sprach- und Kommunikationsfragen.

Das bedeutet nicht, dass internationale Unternehmen überfordert sein müssen. Aber sie brauchen klare Zuständigkeit.

Wer prüft welche Gesellschaft?

Welches Recht ist relevant?

Welche Daten fließen wohin?

Welche Dienstleister sitzen in welchem Land?

Welche Kunden verlangen was?

Internationale Mobilität und internationale Unternehmensstrukturen brauchen digitale Ordnung.

Der Sonderfall darf nicht lähmen

Bei Hartmann entstand zunächst das Gefühl, alles werde kompliziert.

Holding. Ausland. Kunden. Krise. Dienstleister. KI. Versicherung. Beirat.

Seine kaufmännische Leiterin unterbrach: „Wir müssen nicht alles heute lösen. Wir müssen es sichtbar machen.“

Das war die richtige Haltung.

Sonderfälle lähmen, wenn man sie als unüberschaubare Ausnahme behandelt. Sie werden handhabbar, wenn man sie in Prüfungen übersetzt.

Welche Gesellschaft?

Welche Rolle?

Welche Systeme?

Welche Daten?

Welche Kundenanforderungen?

Welche besonderen Pflichten?

Welche offenen Rechtsfragen?

Welche Entscheidung?

Damit wird aus Komplexität Arbeit.

Arbeit ist besser als Nebel.

MEMO

1. Welche Gesellschaften gehören zur Gruppe und welche Rolle spielen sie digital?
2. Gibt es kleine Einheiten mit zentralen Schlüsseln?
3. Ist Cyber Teil der Krisenfrüherkennung?
4. Liefern wir an regulierte oder kritische Kunden?
5. Kommen besondere Anforderungen über Verträge zu uns?
6. Gibt es internationale Datenflüsse oder Dienstleister?

Hartmann sah am Ende auf das Gruppenorganigramm.

Es war voller Markierungen.

Früher hätte ihn das gestört.

Jetzt störte ihn nur noch, dass sie dort nicht früher gestanden hatten.

Die Sonderfälle waren keine Auswege.

Sie waren Hinweise.

Und aus Hinweisen musste nun Gewohnheit werden.

17 | Vom Weckruf zur Gewohnheit

Drei Monate nach dem Anruf vor der Frühschicht war im Unternehmen nicht alles gelöst.

Aber vieles war anders.

Die Geschäftsleitung hatte Cyber als festen Tagesordnungspunkt. Weber führte das Cockpit. Baumann berichtete klarer. Keller kannte Notprozesse. Frau Berger hatte eine Rückrufregel, die sie entlastete. Herr Vogel nutzte KI weiter, aber mit Freigabe und Prüfung. Carola erhielt Beiratsberichte. Der alte Fernwartungszugang von Linie drei war neu geregelt.

Nichts davon sah spektakulär aus.

Genau das war gut.

Gute Unternehmensführung wirkt im Alltag oft unspektakulär.

Vom Projekt zum Rhythmus

Hartmann wollte am Anfang ein Projekt.

Projekt heißt: Start, Plan, Budget, Umsetzung, Abschluss, Haken.

Cyber lässt sich so nicht führen.

Natürlich braucht es Projekte. Einführung von Mehr-Faktor-Authentifizierung. Backup-Modernisierung. Dienstleisterprüfung. KI-Inventur. Notfallübung. Versicherungsreview.

Aber das Thema selbst endet nicht.

Bedrohungen ändern sich. Systeme ändern sich. Mitarbeiter wechseln. Dienstleister kommen und gehen. KI-Funktionen entstehen in bestehender Software. Kundenanforderungen werden schärfer. Versicherer stellen neue Fragen. Gesetze entwickeln sich.

Deshalb muss aus dem Projekt ein Rhythmus werden.

Wie Monatsabschluss.

Wie Liquiditätsplanung.

Wie Qualitätsmanagement.

Wie Arbeitssicherheit.

Nicht ständig dramatisch. Aber verlässlich.

Die vier Routinen

Weber entwickelte vier Routinen.

Erstens: Quartalscockpit.

Die Geschäftsleitung sieht Status, Risiken, Fortschritte und offene Entscheidungen. Keine technische Überladung. Klare Ampel, klare Nachweise, klare Fragen.

Zweitens: Halbjahresübung.

Ein Vorfall wird simuliert. Nicht als Theater, sondern als Probe: Wer ruft wen an? Wo liegt der Plan? Wie kommunizieren wir? Funktioniert die Entscheidungskette?

Drittens: Jahresreview.

Versicherung, Dienstleister, KI-Inventur, Betroffenheitsprüfung, Schulungen, Wiederherstellungstest und Beiratsbericht werden jährlich aktualisiert.

Viertens: Anlassbezogene Prüfung.

Neue Software, neuer Dienstleister, neue KI-Funktion, neuer Großkunde, neue Auslandsgesellschaft, Krise oder Unternehmenskauf lösen eine Prüfung aus.

Damit war Cyber nicht mehr Sondersituation. Es wurde Teil der Unternehmenssteuerung.

Die Rolle der CyberPedia

Hartmann fragte, wie man bei der beweglichen Rechtslage den Überblick behalten solle.

Die Antwort war nicht: durch ein dickes gedrucktes Glossar im ersten Buch.

Die Antwort war: durch ein lebendes Nachschlagewerk.

Die CyberPedia übernimmt die Tiefe. Dort gehören Begriffe, Fristen, Quellen, Prüfungsschritte, Detailhinweise und Aktualisierungen hin. Das Unternehmerhandbuch erklärt, warum und wie die Geschäftsleitung führen muss. Die CyberPedia erklärt, was im Detail zu beachten ist.

Diese Trennung schützt beide Werke.

Das Buch bleibt lesbar.

Die CyberPedia bleibt aktuell.

Ein gedrucktes Buch kann Haltung und Struktur vermitteln. Ein digitales System kann Änderungen aufnehmen, Quellen pflegen und vertiefende Hinweise bereitstellen.

Für Hartmann war das einleuchtend.

Er brauchte im Alltag nicht jeden Paragraphen auf dem Schreibtisch. Er brauchte ein Cockpit, klare Prozesse und die Gewissheit, dass Detailfragen bei Bedarf vertieft werden.

Kultur schlägt Aktionismus

Hartmann merkte, dass die wichtigste Veränderung nicht in der Technik lag.

Sie lag in der Kultur.

Mitarbeiter fragten früher nach, ohne sich zu schämen. Der Vertrieb prüfte KI-Texte. Die IT sprach verständlicher. Die Geschäftsleitung fragte regelmäßiger. Der Beirat bekam Sicht. Dienstleisterzugänge wurden nicht mehr als Nebensache behandelt. Versicherung wurde nicht mehr als Beruhigung, sondern als Vertrag mit Voraussetzungen verstanden.

Das Unternehmen war nicht perfekt.

Aber es war wacher.

Kultur entsteht nicht durch ein Plakat. Sie entsteht durch wiederholtes Verhalten.

Wenn der Geschäftsführer Nachfragen belohnt, fragen Menschen nach.

Wenn der Beirat Cyber ernst nimmt, wird es ernst genommen.

Wenn Wiederherstellungstests wirklich stattfinden, werden Backups nicht nur behauptet.

Wenn KI-Regeln kurz und praktikabel sind, werden sie eher gelebt.

Wenn rote Punkte nicht bestraft, sondern bearbeitet werden, wird das Cockpit ehrlich.

Der Weckruf darf nicht verklingen

Ein Weckruf hat ein Problem.

Man kann danach wieder einschlafen.

Viele Unternehmen erleben einen Vorfall, eine Prüfung, einen Kundenfragebogen oder ein Versicherungsproblem. Dann wird ein paar Wochen intensiv gearbeitet. Ordner entstehen. Maßnahmen werden beschlossen. Schulungen finden statt. Danach drängt der Alltag zurück.

Produktion. Vertrieb. Personal. Liquidität. Kunden. Steuern. Investitionen.

Alles wichtig.

Und genau deshalb braucht Cyber einen Platz im Rhythmus. Nicht, weil es immer das wichtigste Thema ist. Sondern weil es zu wichtig ist, um nur bei Angst aufzutauchen.

Hartmann schrieb in sein Notizbuch:

| „Nicht vergessen, wenn es wieder läuft.“

Das ist vielleicht einer der wichtigsten Sätze des Buches.

MEMO

1. Ist Cyber bei Ihnen Projekt oder Routine?
2. Gibt es ein Quartalscockpit?
3. Werden Notfälle geübt?
4. Wird die KI-Inventur regelmäßig aktualisiert?
5. Werden Versicherungen und Antragsangaben jährlich geprüft?
6. Gibt es eine digitale CyberPedia oder vergleichbare Wissensbasis für Detailfragen?
7. Gibt es eine klare Lotsenfunktion, die beobachtet, ordnet und eskaliert?

Hartmann hatte am Anfang gefragt, was Cyber koste.

Am Ende fragte er anders:

Was sichert es?

Diese Frage veränderte die Diskussion. Denn plötzlich ging es nicht mehr nur um Aufwand, sondern um Substanz.

Und damit wäre diese Reise beinahe zu Ende erzählt. Der Weckruf war zur Gewohnheit geworden, die Ordnung stand, das Unternehmen war wacher als je zuvor.

Aber ein Jahr nach dem Anruf vor der Frühschicht klingelte noch einmal ein Telefon. Diesmal nicht um 05:17 Uhr. Diesmal am Vormittag. Und diesmal ging es nicht um das, was Hartmann verlieren konnte.

Es ging um das, was er noch nicht gehoben hatte.

Teil VI – Der gehobene Schatz

Wie aus Sicherheit Zukunftsfähigkeit wird

18 | Der Anruf am Vormittag

Um 09:40 Uhr klingelte das Telefon. Nicht um 05:17 Uhr. Das ist der Unterschied, um den es in diesem Teil geht.

Es war ein Donnerstag, gut ein Jahr nach dem Morgen, an dem die Bildschirme schwarz geworden waren.

Das Jahr dazwischen war kein spektakuläres gewesen. Es war ein teures gewesen, und ein gründliches.

Hartmann hatte investiert – nicht in ein einzelnes Wundersystem, sondern in viele unspektakuläre Dinge: Mehr-Faktor-Authentifizierung für alle externen Zugänge. Eine modernisierte Backup-Landschaft, deren Wiederherstellung inzwischen zweimal erfolgreich geprobt war. Schulungen, auch für die Geschäftsleitung. Ein Forensik-Retainer, damit im Ernstfall niemand mehr um sechs Uhr morgens Telefonnummern suchen musste. Die Versicherung war neu verhandelt, Antrag und Wirklichkeit stimmten jetzt überein. Der Beirat hatte das alles als Resilienzbudget beschlossen – Carolas Frage dazu war jedes Mal dieselbe gewesen: Welches Risiko reduzieren wir damit?

Und über allem lag das Cockpit. So nannten sie den Nachfolger des roten Ordners: die Übersicht, in der Weber Risiken, Maßnahmen und Nachweise führte – mit ehrlicher Ampel, mit Verantwortlichen, mit Terminen. Quartalsweise ging es durch die Geschäftsleitung, halbjährlich an den Beirat. Am Montag dieser Woche war es turnusgemäß durchgegangen, mit zwei gelben Punkten und einem Beschluss; den Wiederherstellungstest für November hatte Weber terminiert, bevor jemand daran erinnern musste. Es war Routine geworden. Genau das, was Kapitel 17 versprochen hatte.

Was in diesem Cockpit nicht stand, fiel an jenem Donnerstag noch niemandem auf: Es enthielt alles, was das Unternehmen schützte. Es enthielt nichts von dem, was es voranbringen sollte.

Auf dem Display stand der Name des großen Industriekunden.

Hartmann nahm ab und erwartete das Übliche: einen Liefertermin, eine Änderung, vielleicht eine Reklamation. Stattdessen war der Einkaufsleiter selbst am Apparat, Herr Sattler, und Sattler rief nie selbst an.

„Herr Hartmann, keine Sorge, es brennt nichts“, sagte Sattler.
„Im Gegenteil. Ich rufe an, weil wir Sie frühzeitig mitnehmen wollen.“

Hartmann wusste mit dieser Formulierung zunächst noch nichts anzufangen, aber er kannte den Ton. Es war der Ton, in dem große Kunden Dinge ankündigen, die man nicht ablehnen kann.

„Wir stellen unsere Lieferantensteuerung um“, fuhr Sattler fort.
„Ab dem kommenden Jahr wird ein KI-gestütztes System unsere Beschaffung vorbereiten. Es bewertet Angebote vor. Es liest Nachweise aus – Zertifikate, Sicherheitsauskünfte, Auditberichte, Lieferhistorie. Es beobachtet Risiken bei unseren Partnern laufend, nicht mehr einmal im Jahr per Fragebogen. Und es schlägt unseren Einkäufern vor, welche Lieferanten für eine Anfrage überhaupt in Betracht kommen.“

„Es schlägt vor“, wiederholte Hartmann.

„Es schlägt vor. Entscheiden tun Menschen. Aber Sie wissen selbst, wie das ist, Herr Hartmann: Was nicht auf der Vorschlagsliste steht, wird selten entschieden.“

Hartmann schwieg einen Moment.

„Und was heißt das für uns?“

„Das heißt: In sechs Monaten beginnt die Pilotphase. Wir laden unsere wichtigsten Partner ein, ihre Unterlagen in strukturierter Form bereitzustellen. Wer das kann, ist im System von Anfang an sauber abgebildet. Wer es nicht kann, wird vom System so bewertet, wie es eben bewertet, wenn Informationen fehlen.“ Sattler machte eine kleine Pause. „Ich rufe Sie persönlich an, weil Sie uns letztes Jahr nach Ihrem Vorfall so geordnet informiert haben. So etwas merkt man sich. Ich möchte, dass Sie in diesem System gut dastehen.“

Als Hartmann auflegte, blieb er einen Moment sitzen und horchte in sich hinein.

Sein Puls hatte reagiert. Nicht so hart wie damals, um 05:17 Uhr, als Keller sagte: „Wir kommen nicht rein.“ Aber es war dasselbe Organ, das da reagierte. Dieselbe Stelle im Körper, an der Verantwortung Gewicht bekommt.

Dabei hatte niemand gedroht. Niemand wollte Lösegeld. Der Anruf war freundlich gewesen, fast fürsorglich.

Und genau das verstand Hartmann in dieser Minute: Es gibt zwei Arten, ein Unternehmen zu verlieren. Die eine kommt nachts, mit weißem Text auf dunklem Grund. Die andere kommt vormittags, höflich, mit sechs Monaten Vorlauf. Die eine nimmt einem die Daten weg. Die andere nimmt einem die Aufträge weg – nicht mit einem Schlag, sondern Vorschlagsliste für Vorschlagsliste.

Gegen die erste hatte er sich ein Jahr lang gewappnet.

An die zweite hatte er nicht mehr gedacht.

Der Stammtisch

Zwei Wochen später saß Hartmann wieder beim Unternehmerabend. Kalte Platten, warmes Bier, vertraute Gesichter. Petersen war auch da. Petersen ging es gut, das sah man, und es war nicht nur der Anzug.

Aber an diesem Abend sprach nicht Petersen. An diesem Abend sprach Möller, der einen Betrieb für Präzisionsteile führte, zwei Landkreise weiter, und der sonst wenig sagte.

„Krüger hat uns einen Rahmenvertrag weggeschnappt“, sagte Möller. „Wisst ihr, wie? Der hat sein Angebot in vier Tagen abgegeben. Vollständig. Mit allen technischen Nachweisen. Wir haben drei Wochen gebraucht, wie immer. Als unser Angebot ankam, war die Entscheidung durch.“

„Vier Tage“, sagte jemand. „Wie macht der das?“

„Der arbeitet seit einem Jahr mit so einem KI-Partner“, sagte Möller. „Die haben seine ganze Angebotshistorie aufbereitet.“

Sein System schreibt den ersten Entwurf, seine Leute prüfen.
Der Mann hat nicht mehr Ingenieure als ich. Er hat schnellere.“

Hartmann hörte zu und dachte an einen Abend vor gut einem Jahr, am selben Tisch. Er hatte damals einen Satz gesagt, und er erinnerte sich an jedes Wort: Das ist etwas für Konzerne, Petersen. Oder für Leute mit Zeit.

Krüger war kein Konzern. Krüger hatte auch keine Zeit gehabt. Krüger hatte nur früher angefangen.

Petersen sah zu Hartmann hinüber. Er sagte nichts. Er war zu höflich, um es zu sagen.

Das war das Schlimmste daran.

Diesmal kommt kein Erpresser

Halten wir fest, was hier geschieht, denn es ist die Grundlage aller folgenden Kapitel.

Vor einem Jahr lernte Hartmann: Ein Unternehmen muss nicht wichtig aussehen, um angegriffen zu werden. Es muss nur abhängig sein.

Jetzt lernte er die zweite Lektion: Ein Unternehmen muss nichts falsch machen, um zurückzufallen. Es muss nur langsamer sein als die Veränderung um es herum.

Die Deployment-Welle, von der Petersens Berater vor einem Jahr gesprochen hatten – erst die Konzerne, dann, verpackt in Standardbausteine, der Mittelstand –, war keine Prognose mehr. Sie saß am Stammtisch, sie rief vormittags an. Sattlers Einkaufssystem und Krügers Angebotsassistent waren zwei Enden derselben Bewegung: Auf der einen Seite beginnen Kunden, ihre Entscheidungen von KI-Systemen vorbereiten zu lassen. Auf der anderen Seite beginnen Wettbewerber, ihre Leistung mit KI-Systemen zu beschleunigen.

Dazwischen liegt der, der beides für ein Thema von übermorgen hielt.

Das Bemerkenswerte an dieser zweiten Krise: Sie sieht nicht aus wie eine. Es gibt keinen schwarzen Bildschirm, keine Frist, keinen Betrag. Es gibt nur einen freundlichen Anruf und eine verlorene Ausschreibung. Der Schaden hat keine Uhrzeit. Deshalb ist diese Krise in gewisser Weise gefährlicher als die erste: Gegen den Erpresser gibt es einen Notfallplan. Gegen das langsame Unsichtbarwerden gibt es keinen Alarm.

Es sei denn, die Führung baut einen.

Am Abend nach dem Stammtisch schrieb Hartmann drei Sätze in sein Notizbuch, unter den Satz vom letzten Jahr („Nicht vergessen, wenn es wieder läuft“):

„Der Kunde baut ein System, das uns lesen wird. Der Wettbewerber baut ein System, das schneller anbietet. Was bauen wir?“

Am nächsten Morgen bat er Weber, Baumann, Keller und Herrn Vogel für Freitag in den Besprechungsraum. Auf die Tagesordnung schrieb er nicht „KI-Projekt“.

Er schrieb: „Unser Schatz.“

MEMO

1. Welche unserer Kunden stellen Einkauf, Lieferantenbewertung oder Vergabe auf KI-gestützte Systeme um – und woher wüssten wir es?
2. Wie schnell bietet unser schnellster Wettbewerber heute an – und wie schnell wir?
3. Welche unserer Nachweise und Leistungsbeschreibungen sind heute maschinenlesbar auffindbar?
4. Wer im Unternehmen beobachtet diese Marktveränderung – und an wen berichtet er?
5. Behandelt unsere Geschäftsleitung die Chance mit derselben Dringlichkeit, mit der sie nach dem Weckruf das Risiko behandelt hat?

19 | Die Schatzkarte

Am Freitag um 8 Uhr lagen zwei Dinge auf dem Besprechungstisch.

Das eine war die KI-Inventur. Ein Jahr alt, viermal aktualisiert, ordentlich geführt: Welche Werkzeuge sind freigegeben, wer nutzt sie, welche Daten dürfen hinein, wer prüft die Ergebnisse. Ein gutes Dokument. Ein Schutzdokument.

Das andere war ein leeres Blatt.

„Die Inventur sagt, was wir verhindern“, sagte Weber. „Sie sagt nicht, was wir vorhaben. Dafür ist das da.“ Sie schob das leere Blatt in die Mitte.

„Und was soll darauf?“, fragte Keller.

„Die Antwort auf die Frage, die uns vor einem Jahr ein Berater gestellt hat und die wir nie richtig beantwortet haben“, sagte Hartmann. „Welches Wissen besitzen wir, das kein allgemeines KI-Modell hat?“

Es wurde still. Dann fing Keller an, und es war, als hätte jemand einen Hahn aufgedreht.

Die Wartungs- und Störungshistorie aller Linien, bei Linie drei lückenlos seit dem Vorfall, weil sie als erste sauber dokumentiert worden war. Die Angebotsordner seit 1987. Dreißig Jahre Aufträge, Preise und Kalkulationen im ERP. Das Konstruktionsarchiv. Die Reklamationsakten mit vier Jahrzehnten Werkstoffeffahrung. Die Prüfprotokolle der Qualitätssicherung. Und das, was in keinem System lag: Meister Brandts Kopf. Brandt, der in drei Jahren in Rente ging und der als Einziger wusste, warum Linie drei bei feuchtem Wetter anders klang.

Nach einer Stunde war das Blatt voll. Hartmann sah es an und empfand etwas, das er nicht erwartet hatte: Stolz. Es war eine Bestandsaufnahme wie im Archiv an jenem Samstag vor einem Jahr – nur dass diesmal das ganze Führungsteam davor stand.

Dann stellte Baumann die Frage, die den Stolz sortierte.

„Und wie viel davon könnte eine KI heute nutzen?“

Die Ernüchterung

Sie gingen das Blatt Position für Position durch, mit den Fragen aus Kapitel 1, die jetzt, ein Jahr später, endlich ihren Arbeitseinsatz bekamen: Ist es auffindbar? Ist es strukturiert? Ist es aktuell? Ist es qualitätsgesichert? Ist es rechtlich nutzbar? Ist es geschützt?

Weber führte, wie immer, eine Ampel. Und die Ampel wurde nicht grün.

Die Angebotshistorie: vorhanden, aber in drei Systemgenerationen und zwei Nummernkreisen, dazu vierzig Ordner Papier. Gelb, mit Tendenz.

Das Wartungswissen: für Linie drei hervorragend, für die übrigen Linien lückenhaft, für die Altanlagen fast nur in Köpfen. Gelb und rot.

Die Konstruktionsdaten: digital vollständig, aber die Zeichnungsstände vor 2009 waren nie systematisch bereinigt worden. Gelb.

Brandts Erfahrungswissen: nicht dokumentiert. Rot. Mit Ablaufdatum.

„Der Schatz ist da“, sagte Baumann schließlich. „Er ist nur nicht gehoben. Er ist verschüttet.“

Das war der Satz des Vormittags. Und es ist der Befund in fast jedem mittelständischen Unternehmen, das diese Übung ehrlich macht: Das Wissen existiert. Aber es liegt in Formaten, Systemen und Köpfen, die über Jahrzehnte gewachsen sind – gewachsen für Menschen, die wissen, wo etwas liegt. Nicht für Systeme, die es finden sollen.

Hier zeigt sich, warum die Chancen-Diskussion und die Sicherheits-Diskussion dasselbe Fundament haben. Ein Jahr zuvor hatte Hartmann gelernt: Man kann nicht schützen, was man nicht kennt. Jetzt lernte er die Schwester dieses Satzes: Man kann nicht produktiv machen, was man nicht geordnet hat.

Und noch etwas zeigte sich an diesem Vormittag, fast beiläufig, und es ist der eigentliche Grund, warum dieses Kapitel erst jetzt spielen kann und nicht vor einem Jahr: Als die Runde diskutierte, welche Daten ein KI-System sehen dürfte, musste niemand bei null anfangen. Die Zugriffsrollen existierten. Die Dienstleisterakte existierte. Die Freigaberegeln für KI-Werkzeuge existierten. Die Frage „Wer darf was sehen?“ war keine Grundsatzdebatte mehr, sondern ein Blick ins Cockpit.

Vor einem Jahr wäre dieselbe Sitzung an dieser Stelle stecken geblieben – oder schlimmer: Sie wäre darüber hinweggegangen.

Sicherheit war nicht die Bremse gewesen. Sie war das Fundament, auf dem jetzt gebaut werden konnte.

Die Auswahl

Der Nachmittag gehörte der schwierigsten Disziplin: dem Weglassen.

Auf dem Blatt standen elf denkbare Anwendungsfelder. Elf Baustellen gleichzeitig zu eröffnen wäre kein Aufbruch gewesen, sondern Aktionismus – die Chancen-Variante des Fehlers, den dieses Buch bei der Sicherheit schon beschrieben hat.

Frau Weber schlug drei Prüffragen vor, nach denen sortiert wurde: Wo ist der Nutzen messbar? Wo ist die Datenlage am besten? Wo ist das Risiko beherrschbar?

Zwei Felder blieben übrig.

Das erste: das Angebotswissen. Vier Jahrzehnte Angebote, Kalkulationen und technische Auslegungen – und ein Vertrieb, der pro Angebot Tage brauchte, während Krüger in vier Tagen den Rahmenvertrag holte. Nutzen messbar in Durchlaufzeit. Verantwortlich: Herr Vogel.

Das zweite: das Wartungswissen. Beginnend mit Linie drei, deren Historie die beste war, und mit Meister Brandt, dessen Zeit die knappste war. Nutzen messbar in Störungsbehebungszeit. Verantwortlich: Keller.

Dann tat Weber etwas, das auf den ersten Blick nach Verwaltung aussah und auf den zweiten Blick die wichtigste Entscheidung des Tages war. Sie öffnete das Cockpit und legte neben die Maßnahmen-Matrix eine zweite Tabelle an. Gleiche Spalten: Status, Nachweis, Verantwortlicher, nächster Schritt, Termin, Entscheidung der Geschäftsleitung. Nur die Überschrift war anders.

Chancen-Matrix.

„Warum im Cockpit?“, fragte Vogel. „Das ist doch für die Risiken.“

„Das Cockpit ist dafür da, dass Dinge nicht im Alltag verschwinden“, sagte Weber. „Risiken verschwinden im Alltag. Chancen auch.“

Sie hatte recht, und jeder am Tisch wusste es. Das offene Ticket aus Kapitel 14 – „Restore-Test abgebrochen, Wiederholung erforderlich“, sieben Monate unbeachtet – hatte einen Bruder in fast jedem Unternehmen: die Chancen-Idee aus der Strategieklausur, begeistert beschlossen, nie wieder aufgerufen. Beide sterben auf dieselbe Weise. Nicht an Widerspruch. An Dienstagen.

Deshalb gilt für Chancen dieselbe Regel wie für Risiken: Jeder Punkt braucht einen Eigentümer, eine Entscheidung und ein Datum.

MEMO

1. Haben wir je schriftlich beantwortet, welches Wissen wir besitzen, das kein allgemeines Modell hat?
2. Wo liegt dieses Wissen – und in welchem Zustand: auffindbar, strukturiert, aktuell, qualitätsgesichert, rechtlich nutzbar, geschützt?
3. Welches Erfahrungswissen verlässt uns in den nächsten fünf Jahren mit Menschen – und was tun wir bis dahin?
4. Nach welchen Kriterien wählen wir die ersten zwei Anwendungsfälle aus – und was lassen wir bewusst liegen?
5. Wer führt die Chancen-Matrix, und steht sie mit derselben Verbindlichkeit im Cockpit wie die Risiken?

20 | Vierzig Minuten, richtig gemacht

Herr Vogel hatte auf diesen Auftrag ein Jahr gewartet, ohne es zu wissen.

Vor einem Jahr war er der Mann gewesen, der stolz ein Angebot in vierzig Minuten vorgelegt hatte – und dessen KI-Formulierung eine technische Zusicherung enthielt, die nicht haltbar war. Der skandinavische Kunde hatte es gemerkt. Vogel hatte es nicht vergessen. Seither prüfte er jeden KI-Text dreimal, und manchmal, wenn im Vertrieb jemand zu begeistert von einem Werkzeug sprach, wurde er still.

Jetzt saß er bei Hartmann im Büro und bekam die Aufgabe, es richtig zu bauen: einen Angebotsassistenten, der ausschließlich auf den eigenen, freigegebenen Daten des Hauses arbeitet – der Angebotshistorie, den geprüften Spezifikationen, der Preislogik – und der für jede Aussage angibt, woher sie stammt.

Vogel dachte einen Moment nach. Dann sagte er den Satz, der über diesem Kapitel stehen könnte:

„Ich will wieder vierzig Minuten. Aber diesmal will ich wissen, woher jeder Satz kommt.“

Der erste Anlauf scheitert

Es wäre schön, jetzt zu berichten, dass drei Wochen später alles lief.

Es lief nicht.

Der Dienstleister – ausgewählt nach der Lieferantenakte, geprüft nach den Regeln aus Kapitel 10, mit klar begrenztem Datenzugriff – lud die ersten Bestände und lieferte eine ernüchternde Analyse: Rund ein Drittel der Alt-Angebote war ohne verwertbare Struktur. Dieselbe Baugruppe hieß über die Jahre auf vier verschiedene Arten. Preisstände widersprachen sich, weil Sonderkonditionen nie

als solche gekennzeichnet worden waren. Technische Auslegungen steckten in Fließtext, in Anhängen, in gescannten Faxen.

Die Maschine konnte daraus lernen. Aber sie hätte auch die Fehler gelernt. Und eine KI, die aus widersprüchlichen Daten lernt, wird nicht unsicher.

Sie wird überzeugend falsch.

Das war exakt die Lektion, die Vogel vor einem Jahr schmerzhaft gelernt hatte – nur dass die Quelle des Fehlers diesmal nicht das Internet gewesen wäre, sondern das eigene Archiv.

Also wurde drei Wochen lang aufgeräumt. Artikelbezeichnungen vereinheitlicht. Preisstände markiert. Ein Altbestand aussortiert, der mehr verwirrte als half. Es war unglamouröse Arbeit, und sie stand in keinem Prospekt eines KI-Anbieters.

Hartmann fragte in dieser Zeit einmal ungeduldig, wann denn nun „die KI“ komme.

„Sie ist längst da“, sagte Weber. „Wir machen gerade das, was Petersens Berater vor einem Jahr gesagt haben: Wir sortieren die vierzig Ordner. Es gab nie einen Weg daran vorbei. Es gab nur die Frage, ob wir es vor dem Nutzen tun oder nach dem Schaden.“

Der Regelbetrieb

Sechs Wochen nach dem Start legte Vogel das erste Angebot aus dem neuen System vor.

Der Entwurf hatte achtunddreißig Minuten gebraucht. Jede technische Aussage trug einen Verweis: auf ein früheres Angebot, eine geprüfte Spezifikation, ein Prüfprotokoll. Wo die Datenlage nicht reichte, stand kein selbstbewusster Satz, sondern eine Markierung: fachlich zu klären. Vogel prüfte den Entwurf, änderte zwei Positionen, ergänzte eine – und zeichnete ab. Die Regel aus Kapitel 9 galt unverändert und stand jetzt sogar im Fußbereich jedes Entwurfs: Die Maschine formuliert. Der Mensch verantwortet.

Das erste Angebot aus dem System ging – Vogel hatte darauf bestanden – an den skandinavischen Kunden. Diesmal hielt jede Zusage.

Parallel lief Kellers Pilot in der Produktionsabteilung. Das Wartungswissen von Linie drei wurde durchsuchbar gemacht: die Störungshistorie, die Wartungsprotokolle, dazu zwölf lange Gespräche mit Meister Brandt, aufgezeichnet, verschriftlicht, geordnet. Brandt hatte anfangs abgewinkt – „Das steht doch alles in den Berichten“ –, und dann in den Gesprächen Dinge erzählt, die in keinem Bericht standen. Warum Linie drei bei feuchtem Wetter anders klang. Welche Störung harmlos aussah und keine war.

Der Ertrag zeigte sich schneller als beim Vertrieb. Der neue Schichtführer, acht Monate im Haus, stand an einem Samstag vor einer stehenden Anlage, fragte das System und bekam die drei wahrscheinlichsten Ursachen – mit dem Hinweis auf zwei ähnliche Fälle aus den Jahren 2019 und 2023 und dem, was damals geholfen hatte. Aus den eigenen Unterlagen. Nicht aus dem Internet.

Es war fast wörtlich Petersens Beispiel vom Unternehmerabend. Hartmann bemerkte es, als Keller ihm davon erzählte, und sagte nichts dazu.

Manche Pointen muss man nicht aussprechen.

Was im Cockpit ankam

Weber übernahm vier Zahlen in die Chancen-Matrix, und sie bestand darauf, dass es Zahlen waren und keine Adjektive: die Durchlaufzeit je Angebot in Minuten, der Prüfaufwand je Entwurf, die Störungsbehebungszeit an Linie drei, der Anteil des dokumentierten Brandt-Wissens.

Nicht, weil Zahlen alles sagen. Sondern weil wiederkehrende Zahlen Entwicklung zeigen – dieselbe Logik, mit der das Cockpit seit einem Jahr die Sicherheit führte. Ein Chancen-Bericht voller Begeisterung ist so wenig wert wie eine Sicherheits-Ampel voller ungeprüfem Grün.

Und noch etwas gehört in die Bilanz dieses Kapitels, gerade weil es im Alltag unsichtbar blieb: Kein einziges Mal war in diesen Monaten eine Grundsatzdebatte über Datenschutz, Zugriffe oder Freigaben nötig gewesen. Nicht, weil die Fragen unwichtig geworden wären – sondern weil sie beantwortet waren, bevor die Chance anklopfte. Die Freigabe des Dienstleisters: ein Vorgang nach Akte. Die Zugriffsrollen: ein Blick in die bestehende Ordnung. Die Frage, welche Daten das System sehen darf: geregelt in der KI-Richtlinie, die seit einem Jahr galt.

So sieht es aus, wenn aus einem Weckruf Gewohnheit geworden ist: Die Sicherheit tritt nicht mehr als Thema auf. Sie tritt als Handgriff auf.

MEMO

1. Nennt unsere KI Quellen – und sind es unsere eigenen, geprüften?
2. Was hat die erste ehrliche Analyse unserer Datenqualität ergeben – und wer hat die Bereinigung verantwortet?
3. Bleibt der Mensch erkennbar in der Verantwortung, und ist das dokumentiert?
4. Mit welchen wiederkehrenden Kennzahlen messen wir den Nutzen – statt ihn zu behaupten?
5. Welche Sicherheitsfragen mussten wir beim Start neu diskutieren – und welche waren durch bestehende Ordnung bereits beantwortet?

21 | Gefunden werden

Der Brief kam, wie der Brief der Aufsicht vor einem Jahr gekommen war: ohne Drama.

Sattlers Einkaufssystem hatte die Pilotphase begonnen. Hartmann Maschinenbau war eingeladen worden, seine Unterlagen bereitzustellen, und Weber hatte dafür nicht wochenlang gesammelt. Sie hatte den roten Ordner geöffnet – der längst kein Ordner mehr war, sondern das Cockpit – und bereitgestellt, was seit einem Jahr geführt wurde: die Maßnahmen-Matrix mit Nachweisen. Die Schulungsdokumentation. Das Protokoll des letzten erfolgreichen Wiederherstellungstests. Die Lieferantenakte. Die KI-Inventur samt Richtlinie. Den Versicherungsabgleich. Die Incident-Historie, einschließlich des Vorfalls vor einem Jahr – nicht versteckt, sondern eingeordnet: was geschah, was gelernt, was geändert wurde.

Nun kam die Rückmeldung. Hartmann Maschinenbau war als Lieferant der höchsten Verlässlichkeitsstufe eingestuft, vollständig auditierbar, im System bevorzugt vorgeschlagen.

Zwei Absätze weiter unten stand der Satz, der Hartmann länger beschäftigte als die Einstufung selbst. Man habe im Zuge der Pilotphase das Lieferantenportfolio gestrafft. Partner, deren Angaben nicht belegbar oder nicht maschinell auswertbar gewesen seien, würden künftig nur noch nachrangig berücksichtigt.

Hartmann wusste aus dem Markt, wer darunter war: ein Wettbewerber, der bei den letzten drei Ausschreibungen billiger gewesen war als er. Billiger – aber mit Sicherheitsauskünften, die aus Behauptungen bestanden. Das System hatte nicht gefragt, was einer verspricht. Es hatte gefragt, was einer belegt.

Beim nächsten Telefonat sprach Sattler es offen aus.

„Wissen Sie, Herr Hartmann, vor einem Jahr haben Sie unseren Fragebogen bekommen und vermutlich geflucht.“

„Ich habe geflucht“, sagte Hartmann.

„Der Fragebogen war eine Drohung, ich weiß. Beantworten Sie das, sonst prüfen wir andere.“ Sattler lachte kurz. „Jetzt drehen Sie es um: Ihre Antworten sind heute Ihr Vorsprung. Die Hälfte Ihrer Wettbewerber müsste erst ein Jahr aufholen, um in unserem System so auszusehen wie Sie.“

Hartmann legte auf und dachte an einen Satz des Beraters von damals, im Besprechungsraum mit dem zu großen Tisch: Das ist nicht von einer Behörde. Das ist von Ihrem Umsatz.

Der Satz stimmte noch. Er hatte nur die Richtung gewechselt.

Der Beirat dreht die Frage

Im nächsten Quartalsbericht an den Beirat standen zum ersten Mal beide Matrizen nebeneinander: die Maßnahmen-Matrix und die Chancen-Matrix. Dieselbe Disziplin, dieselben Spalten, dieselbe ehrliche Ampel.

Carola blätterte, wie sie immer blätterte. Dann legte sie die Unterlagen hin.

„Vor einem Jahr habe ich euch bei jeder Cyber-Ausgabe gefragt: Welches Risiko reduzieren wir damit?“, sagte sie. „Die Frage bleibt. Aber ab heute stelle ich bei denselben Unterlagen eine zweite: Welchen Wert schaffen wir damit?“

Sie ließ es einen Moment stehen.

„Und ich will beide Antworten in Zahlen. Bei der ersten habt ihr das gelernt. Die zweite üben wir jetzt.“

Aus dem Resilienzbudget, das der Beirat seit einem Jahr kannte, wurde an diesem Tag ein Doppelbudget: Resilienz und Zukunft, gemeinsam dargestellt, gemeinsam entschieden. Nicht, weil die Unterscheidung verschwand – sondern weil die Trennung künstlich geworden war. Die Datenbereinigung aus Kapitel 20: War das Sicherheit oder Produktivität? Die Lieferantenakte, die jetzt Sattlers System überzeugte: Schutz oder Vertrieb? Die Fragen ließen sich nicht mehr sauber sortieren.

Genau das war der Punkt.

Am Ende der Sitzung kam Carola auf ein Thema, das der Beirat seit Jahren beriet und das an diesem Tag eine neue Seite bekam: die Nachfolge.

„Wir haben letztes Jahr festgestellt, dass wir digitale Ordnung übergeben müssen, nicht nur Vermögen“, sagte sie. „Ich ergänze das heute. Wer dieses Unternehmen einmal übernimmt, übernimmt nicht mehr nur Maschinen, Kunden und ein aufgeräumtes Cockpit. Er übernimmt einen gehobenen Schatz – oder einen verschütteten. Das ist ab jetzt Teil jeder Nachfolgediskussion.“

Niemand widersprach. Meister Brandts zwölf Gespräche lagen dokumentiert im System. Das war, ohne dass es je so genannt worden war, die erste Nachfolgeregelung der neuen Art gewesen.

Der Kreis schließt sich

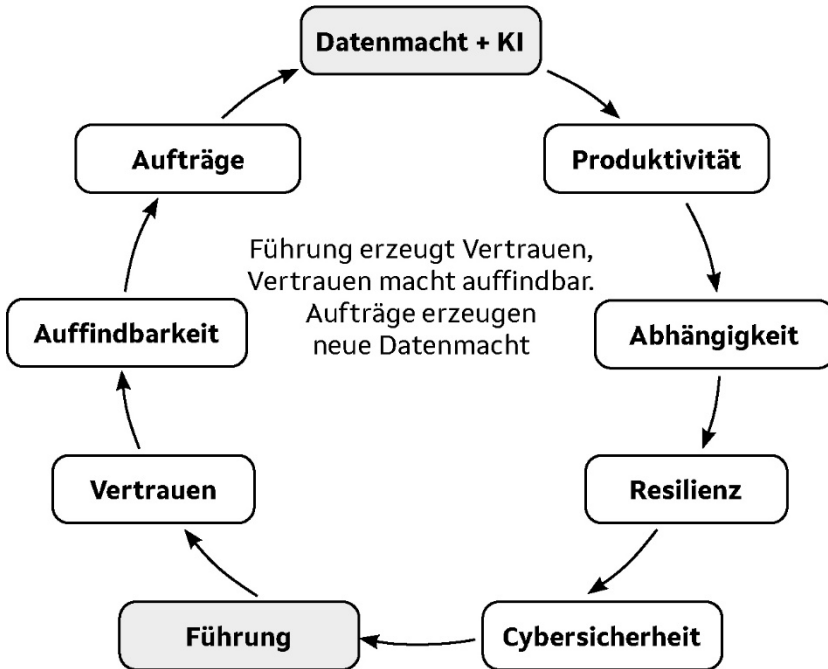
Erinnern wir uns an die Gleichung vom Anfang des Buches: Datenmacht plus KI erzeugt Produktivität. Produktivität erzeugt Abhängigkeit. Abhängigkeit verlangt Resilienz. Resilienz braucht Cybersicherheit. Cybersicherheit braucht Führung.

Ein Jahr lang hat dieses Buch die Kette von links nach rechts erzählt – bis zur Führung, die im Cockpit, im Beirat und in den Routinen ankam.

Dieses Kapitel hat gezeigt, dass die Kette auch rückwärts läuft: Nachweisbare Führung erzeugt Vertrauen. Vertrauen macht auffindbar – für Kunden und zunehmend für deren Systeme. Auffindbarkeit bringt Aufträge. Aufträge erzeugen neue Daten, neue Erfahrung, neue Datenmacht.

Aus der Kette wird ein Kreis. Und ein Unternehmen, das diesen Kreis einmal geschlossen hat, hat etwas, das kein Wettbewerber schnell kopieren kann – nicht, weil die Technik geheim wäre, sondern weil der Kreis Zeit braucht. Krüger hatte ein Jahr Vorsprung beim Anbieten. Hartmann hatte ein Jahr Vorsprung beim Nachweisen. Ab jetzt hatte er beides.

Zwei Ketten verbinden sich zum Kreis



Cybersicherheit war in diesem Kreis nie die Bremse gewesen. Sie war auch nicht nur der Schutz des Schatzes. Sie war – das ist die letzte Wendung dieses Buches – die Eintrittskarte in Märkte, die von Systemen vorsortiert werden: Lieferfähigkeit, Bonität, Versicherbarkeit, Nachfolgefähigkeit, KI-Fähigkeit. Unternehmenssubstanz.

Hartmann hatte vor einem Jahr gefragt, was Cyber kostet.

Dann hatte er gefragt, was es sichert.

Jetzt kannte er die dritte Frage, und sie stand ab diesem Quartal über beiden Matrizen im Cockpit:

Was ermöglicht es?

MEMO

1. Können die KI-Systeme unserer Kunden erkennen und belegen, wofür wir stehen – oder nur unsere Prospekte?
2. Welche unserer Nachweise sind maschinenlesbar bereitgestellt, und wer hält sie aktuell?
3. Behandeln Geschäftsleitung und Beirat Chancen mit derselben Disziplin wie Risiken – Eigentümer, Entscheidung, Datum, Kennzahl?
4. Wird bei Budgetentscheidungen beides gefragt: Welches Risiko reduzieren wir, welchen Wert schaffen wir?
5. Ist unser Schatz übergabefähig – dokumentiert, geordnet, unabhängig von einzelnen Köpfen?

Epilog – Der ruhige Dienstag

Es ist wieder ein Morgen bei Hartmann.

Diesmal klingelt kein Telefon um 05:17 Uhr.

Kein verschlüsseltes ERP. Kein hektischer Anruf aus der Produktion. Keine dunklen Bildschirme. Keine Mitarbeiter, die ratlos in der Halle stehen. Keine fremde Forderung in kaltem Englisch.

Es ist ein Dienstag.

Die Maschinen laufen. Im Versand piept ein Scanner. Die Buchhaltung prüft eine Bankverbindung und ruft zur Sicherheit zurück. Der Vertrieb verschickt ein Angebot, dessen Entwurf in achtunddreißig Minuten aus der eigenen Angebotshistorie entstanden ist – jede Zusicherung mit Quelle, von Herrn Vogel geprüft und abgezeichnet. In der Halle fragt der Schichtführer das Wartungssystem nach einer Unregelmäßigkeit an Linie drei und bekommt die Antwort aus den eigenen Protokollen, in Minuten. Baumann meldet, dass der Wiederherstellungstest funktioniert hat. Weber aktualisiert das Cockpit – die Ampel der Maßnahmen und, daneben, die Ampel der Chancen. Carola bekommt den Beiratsbericht. Und in der Post liegt die Bestätigung des großen Kunden: höchste Verlässlichkeitsstufe, bevorzugt vorgeschlagen.

Thomas Hartmann sitzt in seinem Büro.

Der Kaffee ist noch heiß.

Das klingt unspektakulär.

Genau das ist der Erfolg.

Gute Vorsorge hat selten Applaus

Niemand applaudiert für eine Krise, die nicht eskaliert.

Kein Kunde schreibt eine Dankeskarte, weil Ihr Backup sauber getestet wurde. Kein Mitarbeiter feiert, weil eine Phishing-Mail gemeldet und gestoppt wurde. Kein Beirat hält eine Rede, weil ein

Dienstleisterzugang rechtzeitig geschlossen wurde. Kein Versicherer gratuliert, weil Antrag und Wirklichkeit zusammenpassen.

Gute Vorsorge ist oft leise.

Sie verhindert nicht jedes Problem. Aber sie verhindert, dass aus jedem Problem eine Katastrophe wird.

Das ist unternehmerisch wertvoll.

Was Hartmann gelernt hat

Hartmann ist am Ende dieses Buches kein IT-Experte.

Das soll er auch nicht sein.

Ein Unternehmen braucht keine Geschäftsführer, die nebenbei Administratoren werden. Es braucht Geschäftsführer, die wissen, was sie führen müssen.

Hartmann denkt heute anders.

Früher fragte er: „Warum sollten die uns angreifen?“

Heute fragt er: „Welche Abhängigkeiten machen uns verwundbar?“

Früher sagte er: „Das macht die IT.“

Heute sagt er: „Die IT bereitet vor. Die Geschäftsleitung entscheidet und überwacht.“

Früher glaubte er: „Wir haben eine Versicherung.“

Heute fragt er: „Stimmen Antrag, Wirklichkeit und Obliegenheiten überein?“

Früher war KI ein nützliches Werkzeug im Vertrieb.

Heute ist KI ein geregelter Teil der Unternehmensorganisation.

Früher war Dokumentation Bürokratie.

Heute ist sie Nachweis von Sorgfalt.

Und früher fragte er, was das alles kostet.

Heute fragt er, was es ermöglicht.

Der wichtigste Wandel liegt nicht in einer einzelnen Maßnahme. Er liegt in der Haltung.

Hartmann hat aufgehört, Cyber als Störung seiner eigentlichen Arbeit zu sehen.

Er sieht es als Teil seiner eigentlichen Arbeit.

Was Unternehmer übergeben

Dieses Buch richtet sich besonders an Unternehmer und Unternehmerfamilien, weil dort Verantwortung oft generationenübergreifend gedacht wird.

Wer ein Unternehmen übergibt, übergibt heute mehr als Maschinen, Immobilien, Kunden, Marken und Verträge.

Er übergibt Daten.

Systeme.

Zugänge.

Digitale Prozesse.

KI-Werkzeuge.

Versicherungsstrukturen.

Dienstleisterbeziehungen.

Nachweise.

Oder Lücken.

Die nächste Generation erbt nicht nur Vermögen. Sie erbt auch digitale Ordnung oder digitales Chaos.

Das klingt hart. Aber es ist gestaltbar.

Ordnung kann geschaffen werden. Risiken können sichtbar gemacht werden. Prozesse können geübt werden. Menschen können geschult werden. KI kann geregelt werden. Versicherungen können geprüft werden. Beiräte können fragen. Geschäftsleitungen können führen.

Nicht perfekt. Aber besser.

Die emotionale Rendite

Unternehmer rechnen.

Investition, Rendite, Aufwand, Nutzen, Risiko.

Das ist richtig. Aber nicht jede Rendite steht in der Bilanz.

Es gibt eine Rendite auf Schlaf.

Eine Rendite auf Ruhe.

Eine Rendite auf die Fähigkeit, am Sonntagabend nicht an ein offenes Kellerfenster im digitalen Haus zu denken.

Diese Rendite entsteht nicht, weil nichts passieren kann. Sie entsteht, weil man weiß: Wir haben das Vernünftige getan. Wir kennen unsere wichtigsten Risiken. Wir haben Zuständigkeiten. Wir haben Nachweise. Wir haben geübt. Wir wissen, wen wir anrufen. Wir wissen, was wir nicht tun dürfen.

Das nimmt nicht jedes Risiko weg.

Aber es nimmt das Gefühl, dem Risiko blind ausgeliefert zu sein.

Der ruhige Dienstag ist kein Zufall

Am Anfang dieses Buches stand ein Anruf.

Am Ende steht ein ruhiger Dienstag.

Dazwischen liegen keine Wunder. Keine perfekte Sicherheit. Keine technische Erlösung. Keine Garantie.

Dazwischen liegen Führung, Fragen, Entscheidungen, Nachweise, Schulungen, Übungen, KI-Regeln, Lieferantenprüfungen, Versicherungsabgleich und ein Cockpit. Und, seit diesem Jahr: eine Schatzkarte, eine Chancen-Matrix und ein Schatz, der arbeitet.

Das ist weniger glamourös als viele Sicherheitsversprechen.

Aber es ist belastbarer.

Der ruhige Dienstag ist kein Zufall.

Er ist das Ergebnis guter Vorbereitung.

Und er ist mehr als die Abwesenheit von Unglück. Der ruhige Dienstag ist kein Stillstand. Er ist der Tag, an dem ein Unternehmen ungestört an seiner Zukunft arbeitet.

Schluss

Vielleicht lesen Sie dieses Buch, weil bereits etwas passiert ist.

Vielleicht, weil ein Kunde gefragt hat.

Vielleicht, weil ein Versicherer nachhakt.

Vielleicht, weil Ihr Beirat wissen will, wie gut Ihr Unternehmen vorbereitet ist.

Vielleicht auch nur, weil Sie den Satz „Wir sind doch kein Krankenhaus“ schon einmal gehört oder selbst gesagt haben.

Dann hat dieses Buch seinen Zweck erfüllt, wenn Sie nach der letzten Seite nicht in Angst handeln, sondern in Ordnung.

Nicht jeder Angriff lässt sich verhindern.

Aber viele schlechte Verläufe lassen sich vorbereitend vermeiden.

Der beste Zeitpunkt dafür ist selten der Moment der Krise.

Der beste Zeitpunkt ist vorher.

Dieses Buch wünscht Ihnen diesen vorherigen Zeitpunkt.

Und es wünscht Ihnen den ruhigen Dienstag.

Das Führungsfragen-Register

Vom Buch zum Führungsinstrument – das Jahresprogramm für Ihre Geschäftsleitung

Sie haben dieses Buch bis hierher gelesen. Die Quintessenz ist eindeutig: Cybersicherheit ist Chefsache. Die naheliegende Frage lautet jetzt: Was heißt das am Montag?

Dieses Register ist die Antwort. Es versammelt die Führungsfragen aus allen Kapiteln dieses Buches – zusammengeführt, von Doppelungen befreit und so geordnet, dass Sie damit arbeiten können. Denn dieses Buch hat eine These, und es wäre unglaublich, wenn es sie nur erzählte: Führung heißt, die richtigen Fragen zu stellen, Nachweise zu verlangen und einen Rhythmus zu bauen. Ab dieser Seite hört das Buch auf zu erzählen und fängt an zu arbeiten.

So verwenden Sie es: Fünf Blöcke, ein Jahr. Nehmen Sie einen Block pro Quartal in Ihre Leitungssitzung – erstes Quartal Ready, zweites Souverän, drittes Widerstandsfähig, viertes Compliant – und den Zukunfts-Block in Ihre Strategieklausur. Nach einem Jahr haben Sie jede Frage dieses Buches einmal beantwortet. Dann beginnt der Kreis von vorn, und Sie vergleichen die Fortschritte.

Jede Frage trägt drei Felder, und sie sind wörtlich die Logik des Cockpits aus Kapitel 14: eine ehrliche Ampel (grün heißt belegt, nicht beruhigt), einen Verantwortlichen und ein Datum. Eine Frage ohne Eigentümer und Termin ist keine Entscheidung, sondern ein guter Vorsatz – und Sie wissen ebenfalls aus Kapitel 14, wie gute Vorsätze enden: nicht an Widerspruch, an Dienstagen.

Hinter jeder Frage steht der Verweis auf das Kapitel, in dem Thomas Hartmann sie durchlebt hat. Wenn Sie bei einer Frage unsicher sind, lesen Sie die Szene noch einmal – Sie werden die Antwort anders geben.

Schreiben Sie in dieses Buch. Dafür ist es gemacht.

Ready – Wissen wir, wo wir stehen?

Bestandsaufnahme vor allem anderen: Systeme, Daten, Zugänge, Dienstleister, Pflichten. Hier beginnt Hartmanns Weg – und hier beginnt Ihrer. Empfohlen für die Leitungssitzung im ersten Quartal. Rot indiziert, dass die Frage noch nicht angegangen wurde oder es dringenden Handlungsbedarf gibt. Gelb bedeutet: Wir befassen uns mit der Aufgabe. Grün heißt: Antwort ist da und dokumentiert und es besteht kein weiterer Handlungsbedarf.

R1 • Welche digitalen Systeme sind für unsere Lieferfähigkeit unverzichtbar – und wie lange überleben wir ohne sie? (Kap. 4, 7)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R2 • Welche Daten wären kritisch, wenn sie verschlüsselt, gestohlen oder veröffentlicht würden? (Kap. 4)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R3 • Was macht unser Unternehmen angreifbar, abhängig oder prüfpflichtig – Geschäftsmodell, Kundenstruktur, Lieferkette? (Kap. 4, 6)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R4 • Kennen wir jeden Zugang von außen in unsere Systeme – einschließlich Fernwartung – und ist er abgesichert? (Kap. 10)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R5 • Welche Dienstleister haben Zugriff auf Systeme, Daten oder kritische Prozesse – und führen wir über sie eine Akte? (Kap. 10)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R6 • Welche KI-Werkzeuge sind heute im Haus im Einsatz – auch die, die niemand freigegeben hat? (Kap. 9)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R7 • Welche Unternehmensdaten fließen in KI-Werkzeuge – und dürfen sie das? (Kap. 9)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R8 • Wer trägt bei uns die Verantwortung für Informationssicherheit – und weiß die Person das? (Kap. 5, 8)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R9 • Wann haben wir zuletzt ein ehrliches Lagebild verlangt – ohne Beschönigung, mit Ampel? (Kap. 5, 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

R10 • Sind wir von NIS-2 direkt betroffen, über die Lieferkette – oder beides? (Kap. 6)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Souverän – Führen wir im Ernstfall?

Wenn es brennt, ist nicht die Technik gefragt, sondern die Spitze. Diese Fragen entscheiden, ob Sie um 05:17 Uhr führen oder getrieben werden. Empfohlen für das zweite Quartal.

S1 • Wer ruft wen an, wenn heute Nacht die Bildschirme schwarz werden – und existiert diese Liste auf Papier? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S2 • Wer führt den Krisenstab, wer entscheidet, wer kommuniziert – und wer vertritt wen? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S3 • Kennen wir unsere Meldeuhren – Aufsicht, Datenschutz binnen 72 Stunden, Versicherer unverzüglich? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S4 • Haben wir die Lösegeldfrage einmal in Ruhe durchdacht – bevor sie uns nachts gestellt wird? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S5 • Wissen unsere Mitarbeiter, was sie im Ernstfall tun und lassen sollen – und was sie nach außen sagen? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S6 • Gibt es für Zahlungs- und Kontoänderungen eine Rückrufregel über einen zweiten Kanal – ohne Ausnahme, auch für den Chef? (Kap. 8)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S7 • Können unsere Führungskräfte einen Vorfall führen – haben sie es geübt, nicht nur gelesen? (Kap. 8, 17)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S8 • Behandeln wir Fehler als Meldeanlass oder als Schuldfrage – traut sich jemand, um 22 Uhr Alarm zu schlagen? (Kap. 8)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

S9 • Sind Forensik und rechtliche Begleitung vorab vereinbart – oder suchen wir im Ernstfall Telefonnummern? (Kap. 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Widerstandsfähig – Stecken wir das weg?

Resilienz heißt nicht, dass nichts passiert. Sie heißt, dass Sie nicht planlos werden, wenn etwas passiert – und dass der Betrieb wieder anläuft. Empfohlen für das dritte Quartal.

W1 • Wann wurde unsere Wiederherstellung zuletzt erfolgreich geprobt – nicht das Backup, die Wiederherstellung? (Kap. 6, 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W2 • Wie lange dauert der Wiederanlauf unserer kritischen Systeme – Stunden, Tage, Wochen – und wer hat das gemessen? (Kap. 12, 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W3 • Sind unsere Backups vom Netz getrennt und gegen Manipulation geschützt? (Kap. 5, 12)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W4 • Ist jeder Zugang von außen mit einem zweiten Faktor gesichert – ohne historische Ausnahmen? (Kap. 5, 17)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W5 • Welche offenen Tickets und bekannten Lücken sind älter als drei Monate – und wer hat entschieden, dass das so bleibt? (Kap. 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W6 • Üben wir den Ernstfall regelmäßig – mit Terminen im Kalender statt guten Vorsätzen? (Kap. 17)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W7 • Sind die Obliegenheiten unserer Versicherung in den Notfallplan eingebaut – damit wir sie im Chaos nicht verletzen? (Kap. 13)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

W8 • Verkraften wir den Ausfall unseres wichtigsten Dienstleisters – gibt es einen geprüften Plan B? (Kap. 10)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Compliant – Können wir es belegen?

Wenn morgen der Fragebogen Ihres größten Kunden käme – oder der Brief der Aufsicht: Was könnten Sie vorlegen? Nachweis ist Substanz. Empfohlen für das vierte Quartal.

C1 • Welche Nachweise könnten wir binnen 48 Stunden vorlegen – Beschlüsse, Schulungen, Tests, Prüfungen? (Kap. 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C2 • Stimmen die Angaben in unserem Versicherungsantrag mit der Wirklichkeit überein – heute, nicht bei Abschluss? (Kap. 13)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C3 • Ist jede Schulung dokumentiert – auch die der Geschäftsleitung selbst? (Kap. 5, 8)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C4 • Werden unsere Sicherheitsentscheidungen protokolliert – auch die bewussten Nein-Entscheidungen mit Begründung? (Kap. 11, 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C5 • Führen wir das Cockpit mit ehrlicher Ampel – und in welchem Rhythmus berichtet es an Leitung und Beirat? (Kap. 14, 15)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C6 • Kennt unser Beirat das Cyber-Lagebild – und sind Zustimmungsvorbehalte und Budget geklärt? (Kap. 15)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C7 • Deckt unsere Cyber-Police die Risiken, die wir wirklich haben – einschließlich CEO-Fraud? (Kap. 13)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C8 • Wissen wir, welche Pflichten unsere Kunden vertraglich an uns durchreichen – und können wir sie belegen? (Kap. 10)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C9 • Ist geregelt und dokumentiert, dass bei KI-Ergebnissen der Mensch prüft und verantwortet? (Kap. 9)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

C10 • Würde unsere Dokumentation eine Anfrage der Aufsicht überstehen – ohne Wochenendeinsatz? (Kap. 6, 14)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Zukunftsfähig – Arbeitet unser Schatz?

Sicherheit war die Voraussetzung. Jetzt kommt die Ernte: der eigene Datenschatz, die ersten Anwendungsfälle, die Auffindbarkeit für die Systeme Ihrer Kunden. Empfohlen für die Strategieklausur.

Z1 • Welches Wissen besitzen wir, das kein allgemeines KI-Modell hat – und haben wir es je schriftlich beantwortet? (Kap. 1, 19)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z2 • In welchem Zustand ist der Schatz auffindbar, strukturiert, aktuell, qualitätsgesichert, rechtlich nutzbar, geschützt? (Kap. 19)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z3 • Welche Kunden stellen Einkauf und Lieferantenbewertung auf KI-Systeme um – und woher wüssten wir es? (Kap. 18)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z4 • Wie schnell bietet unser schnellster Wettbewerber heute an – und wie schnell wir? (Kap. 18)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z5 • Welche zwei Anwendungsfälle haben das beste Verhältnis aus Nutzen, Datenlage und Risiko? (Kap. 19)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z6 • Führen wir Chancen mit derselben Disziplin wie Risiken – Eigentümer, Entscheidung, Datum, Kennzahl? (Kap. 19, 21)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z7 • Nennt unsere KI Quellen – und sind es unsere eigenen, geprüften? (Kap. 20)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z8 • Welches Erfahrungswissen verlässt uns in den nächsten fünf Jahren mit Menschen – und was tun wir bis dahin? (Kap. 19)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z9 • Sind unsere Nachweise für die KI-Systeme unserer Kunden lesbar – existieren wir in deren Vorauswahl? (Kap. 21)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z10 • Fragen wir bei jeder Ausgabe beides: Welches Risiko reduzieren wir – und welchen Wert schaffen wir? (Kap. 15, 21)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Z11 • Ist unser Schatz übergabefähig – dokumentiert, geordnet, unabhängig von einzelnen Köpfen? (Kap. 21)

Status: ☐ grün ☐ gelb ☐ rot

Verantwortlich _____ Bis wann _____

Teil VII – Anhang

*Recht und Nachweis
Zahlen, Fälle und Quellen*

Anhang A | Recht und Nachweis

Die folgenden Seiten greifen 13 Rechtsthemen auf, die in diesem Buch eine Rolle spielen – von der persönlichen Haftung der Geschäftsleitung bis zur 72-Stunden-Meldung. Jedes Thema steht hier auf einer Seite: das Prinzip, nicht der Paragraph.

Denn ein gedrucktes Buch hat eine ehrliche Schwäche: Rechtsstände ändern sich, Papier nicht. Fristen werden verschoben, Schwellenwerte angepasst, Urteile gesprochen. Deshalb nennt jede Seite dieses Anhangs den Stand ihres Wissens – und den Ort, an dem dieser Stand gepflegt wird: die CyberPedia, eine frei zugängliche Rechts- und Wissensdatenbank der Initiative **Cyber-schutzengel**, an der der Autor beteiligt ist. Das sei offen gesagt, damit Sie es nicht suchen müssen. Verwendet wird sie hier aus einem einzigen Grund: Sie wird aktualisiert, dieses Buch nicht.

Sie bleiben dabei unabhängig. Jede Seite nennt neben der CyberPedia auch die Primärquelle – das Gesetz, das Urteil, die amtliche Fundstelle. Der Weg an uns vorbei steht Ihnen jederzeit offen. Die Auswahl der Themen ist exemplarisch, nicht vollständig; vollständig ist nur der Anspruch, dass jede Aussage hier belegbar ist.

Alle Angaben in diesem Anhang entsprechen dem Rechtsstand bei Drucklegung im August 2026. Sie ersetzen keine Rechtsberatung im Einzelfall.

Organhaftung – Das Unternehmen als Kläger

Was gilt

Die Innenhaftung ist der Weg, auf dem ein Cybervorfall das Privatvermögen der Geschäftsleitung erreicht. Nicht der Angreifer klagt, nicht der Staat – die eigene Gesellschaft fordert den Schaden zurück, gestützt auf § 43 GmbHG oder § 93 AktG. § 38 Abs. 2 BSIG verklammert diese alte gesellschaftsrechtliche Haftung seit Dezember 2025 ausdrücklich mit den Cyber-Pflichten des BSIG. Ein gesetzliches Höchstmaß gibt es nicht.

Der Maßstab ist der ordentliche und gewissenhafte Geschäftsleiter – objektiv, nicht nach persönlichem Können. Er kennt die wesentlichen Cyber-Risiken seines Hauses, wählt angemessene Maßnahmen, delegiert die Ausführung und behält die Überwachung. Die Business Judgement Rule schützt dabei nur die informierte Ermessensentscheidung, etwa die Verteilung des Sicherheitsbudgets – nie das Ob gesetzlicher Pflichten. Wer die Mindestmaßnahmen des § 30 BSIG gar nicht umsetzt, hat kein Ermessen, auf das er sich berufen könnte.

Wen es trifft

Geschäftsführer und Vorstände haften ihrer eigenen Gesellschaft – auch dann, wenn die Einrichtung gar nicht unter NIS-2 fällt, denn die Pflicht zu einem angemessenen Compliance-System gilt nach der Neubürger-Rechtsprechung rechtsformübergreifend. Mehrere Geschäftsleiter haften gesamtschuldnerisch. Die Verjährung läuft fünf Jahre, bei börsennotierten Aktiengesellschaften zehn – so lange muss der Nachweisbestand halten.

Wo es im Buch spielt

Kapitel 5 („Das macht doch unsere IT“ – Aufgabe und Verantwortung sind nicht dasselbe) und Kapitel 11 (die fünf Haftungsebenen).

Der Haken

Der Haken heißt Beweislastumkehr. Ist streitig, ob die Sorgfalt eingehalten wurde, muss nicht die Gesellschaft die Pflichtverletzung beweisen – die Geschäftsleitung muss ihre Pflichterfüllung beweisen (§ 93 Abs. 2 Satz 2 AktG, für die GmbH nach gefestigter BGH-Linie entsprechend). Ohne Dokumentation steht sie mit leeren Händen in einem Prozess, dessen Beweislast sie trägt.

Delegation ist erlaubt, Enthftung durch Delegation nicht. Auswahl, Vertrag und laufende Überwachung des Dienstleisters bleiben eigene Pflicht der Geschäftsleitung – ein ungelesener Prüfbericht im Archiv enthaftet nicht.

Was sich zuletzt bewegt hat

Das BSIG mit der Haftungsbrücke des § 38 Abs. 2 gilt seit dem 6. Dezember 2025. Am 19. November 2025 hat der BGH den Wissenslichkeitsausschluss der D&O eng gezogen (IV ZR 66/25): Der Versicherer muss die positive Kenntnis der konkret verletzten Pflicht beweisen. Schon am 18. Dezember 2024 hatte der BGH insolvenzbezogene D&O-Klauseln gekippt (IV ZR 151/23). Ob Verbandsgeldbußen auf Organe abgewälzt werden können, liegt seit der BGH-Vorlage vom 11. Februar 2025 (KZR 74/23) beim EuGH. Und das Bundeslagebild Cybercrime meldete am 12. Mai 2026 für das Jahr 2025 insgesamt 1.041 angezeigte Ransomware-Angriffe – zehn Prozent mehr als im Vorjahr.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-1

Primärquellen: § 38 Abs. 2, § 30 BSIG; § 43 GmbHG; §§ 91, 93 AktG (gesetze-im-internet.de) · BGH, Urt. v. 19.11.2025 – IV ZR 66/25 (ECLI:DE:BGH:2025:191125UIVZR66.25.0); BGH, Urt. v. 18.12.2024 – IV ZR 151/23; BGH, Beschl. v. 11.02.2025 – KZR 74/23 · LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 („Siemens/Neubürger“)

CyberPedia-Grundlage: Fachartikel „Die Innenhaftung der Geschäftsleitung nach § 38 Abs. 2 BSIG i. V. m. § 43 GmbHG und § 93 AktG“ und „Die Überwachungspflicht der Geschäftsleitung“ (Rechts-/Redaktionsstand 26.06.2026, Version 1.7) · Glossar: Innenhaftung, Business Judgment Rule (Normstand 10.07.2026), Sorgfaltspflicht (Normstand 11.07.2026)



NIS-2, Leitungspflicht und § 38 BSIG

Was gilt

§ 38 BSIG bündelt drei Pflichten der Geschäftsleitung in einer Norm: die Risikomanagementmaßnahmen nach § 30 BSIG umsetzen, ihre Umsetzung überwachen und sich selbst regelmäßig schulen. Alle drei gelten seit dem 6. Dezember 2025 – eine Übergangsfrist gibt es nicht. Wer nur an die Schulung denkt, übersieht zwei Drittel der Norm; der eigentliche Sorgfalts-Hebel ist die Überwachung. Verletzt die Geschäftsleitung Umsetzung oder Überwachung, führt § 38 Abs. 2 BSIG als Brücke direkt in die persönliche Innenhaftung nach § 43 GmbHG oder § 93 AktG.

Daneben läuft das Pflichtenprogramm der Einrichtung: Registrierung binnen drei Monaten nach Erfassung, bei erheblichen Sicherheitsvorfällen die Meldekaskade – Erstmeldung binnen 24 Stunden, bestätigende Meldung binnen 72 Stunden, Abschlussmeldung nach einem Monat. Jede dieser Fristen ist ein eigener Bußgeldtatbestand, keine Formalie. Auch die Dokumentation der Maßnahmen ist ein eigener Tatbestand neben der Sachpflicht.

Wen es trifft

Betroffen sind besonders wichtige und wichtige Einrichtungen nach § 28 BSIG: besonders wichtig ab 250 Mitarbeitern oder über 50 Millionen Euro Umsatz und zugleich über 43 Millionen Euro Bilanzsumme, wichtig schon ab 50 Mitarbeitern oder jeweils über zehn Millionen Euro Umsatz und Bilanzsumme. Mitgerechnet werden nach der EU-Empfehlung 2003/361/EG auch Partner- und verbundene Unternehmen. Geschäftsleitung ist, wer nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung berufen ist.

Wo es im Buch spielt

Kapitel 6 („Es kommt keine Post vom Amt“ – genau darum) und Kapitel 14 (das Cockpit als Antwort auf die Nachweisfrage).

Der Haken

Die Schulungspflicht steht in Absatz 3 – und fällt damit nicht unter die Haftungsbrücke des Absatzes 2. Haftungsfrei ist sie deshalb nicht: Ihre Verletzung läuft über die allgemeine gesellschaftsrechtliche Sorgfaltspflicht, und „regelmäßig“ ist die einzige Frequenzvorgabe des Gesetzes.

Das Bußgeld trifft die Einrichtung: bis zu zehn Millionen Euro (besonders wichtig) beziehungsweise sieben Millionen Euro (wichtig); ab 500 Millionen Euro Gesamtumsatz kann die Behörde stattdessen bis zu 2 beziehungsweise 1,4 Prozent des weltweiten Gesamtumsatzes ansetzen. Die schärfste persönliche Sanktion steht in § 61 Abs. 9 BSIG: Bei besonders wichtigen Einrichtungen kann die Aufsicht unzuverlässigen Geschäftsleitungen als letztes Mittel die Ausübung der Leitungstätigkeit vorübergehend untersagen. Ob das über § 62 BSIG auch Geschäftsleitungen wichtiger Einrichtungen treffen kann, ist eine offene Auslegungsfrage.

Was sich zuletzt bewegt hat

Das BSIG wurde am 2. Dezember 2025 ausgefertigt, trat am 6. Dezember 2025 in Kraft und wurde durch das KRITIS-Dachgesetz vom 11. März 2026 mit Wirkung zum 17. März 2026 geändert. Für Einrichtungen, die schon bei Inkrafttreten erfasst waren, lief die Registrierungsfrist am 6. März 2026 ab – wer sich nicht registriert hat, ist seither in Verzug. Behördliche Nachweisanordnungen kommen zeitversetzt: frühestens ab dem 6. Dezember 2028, für zugelassene Krankenhäuser grundsätzlich ab dem 6. Dezember 2030. Eine im Referentenentwurf vorgesehene Klausel, die Verzicht und Vergleich bei Ansprüchen aus § 38 Abs. 2 BSIG verboten hätte, wurde vor der Verkündung gestrichen.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-2

Primärquellen: §§ 28, 30, 32, 33, 38, 61, 62, 65 BSIG (BSIG v. 02.12.2025, BGBl. 2025 I Nr. 301, zuletzt geändert durch Art. 4 G v. 11.03.2026, BGBl. 2026 I Nr. 66) · § 30 OWiG · § 43 GmbHG; § 93 AktG · Richtlinie (EU) 2022/2555 (ABl. L 333 v. 27.12.2022) · Empfehlung 2003/361/EG

CyberPedia-Grundlage: Fachartikel „Die NIS-2-Pflichten der Geschäftsleitung nach § 38 BSIG“ (Stand Mai 2026), „Haftung und Sanktionen unter NIS-2“ (Änderungsstand 11.03.2026 berücksichtigt), „Anwendungsbereich und Schwellenwerte“ (Stand 09.06.2026), „Die Verbandsgeldbuße“ (Stand 26.06.2026, V1.5), „Tätigkeitsverbot“ (Stand 27.06.2026, V1.10)



Schulungspflichten – Lernen muss belegbar sein

Was gilt

Cybersicherheit kann man nicht delegieren – Lernen auch nicht. § 38 Abs. 3 BSIG verpflichtet die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen, regelmäßig selbst an Schulungen teilzunehmen. Ziel ist, dass die Leitung Cyber-Risiken erkennen und bewerten kann und versteht, was Risiken und Gegenmaßnahmen für die eigenen Dienste bedeuten. Die Pflicht trifft jedes Geschäftsleitungsmitglied persönlich und steht neben der Umsetzungs- und Überwachungspflicht aus § 38 Abs. 1 BSIG.

Für die Belegschaft gilt das Prinzip auf der zweiten Ebene: Grundlegende Schulungen und Sensibilisierungsmaßnahmen sind Mindestmaßnahme Nummer 7 des § 30 Abs. 2 BSIG – Zielgruppen sind aus Rollen, Zugriffen und Risikosituationen abzuleiten. Dazu kommt die KI-Schiene: Art. 4 KI-VO verlangt seit dem 2. Februar 2025 ein ausreichendes Maß an KI-Kompetenz für das Personal und für Dritte, die im Auftrag mit KI-Systemen arbeiten – eine Bemühenspflicht „nach besten Kräften“, abgestuft nach Einsatzkontext.

Wen es trifft

Die Leitungsschulungspflicht trifft jede natürliche Person, die Geschäftsleitung im Sinne des § 2 Nr. 13 BSIG ist, sofern die Einrichtung unter § 28 BSIG fällt. Prokuristen und Aufsichtsräte sind nicht direkt erfasst, sollten laut CyberPedia aber in den Schulungsplan einbezogen werden. Für Telekommunikation, Energie und DORA-Finanzunternehmen gelten Bereichsausnahmen mit inhaltsgleichen Parallelpflichten (§ 165 TKG, § 5e EnWG, Art. 5 DORA). Die KI-Kompetenz-Pflicht trifft Anbieter und Betreiber von KI-Systemen unabhängig davon, ob NIS-2 greift.

Wo es im Buch spielt

Kapitel 5 (die Schulbank der Leitung), Kapitel 8 (Schulung ist kein Ereignis), Kapitel 14 und 17 (Rhythmus statt Einmalaktion).

Der Haken

„Regelmäßig“ definiert das Gesetz nicht. Die Gesetzesbegründung (BT-Drs. 21/1501) nennt Schulungen mindestens alle drei Jahre; die BSI-FAQ nennt mindestens vier Stunden in drei Jahren – und warnt zugleich, dass das in den allermeisten Fällen nicht reicht. Wer gar keinen dokumentierten Rhythmus vorweisen kann, riskiert, dass die Aufsicht die Erfüllung der Pflicht verneint.

Der zweite Haken ist die Beweislast: Im Innenhaftungsprozess muss die Geschäftsleitung darlegen, dass sie ihre Pflicht erfüllt hat. Eine bloße Anwesenheitsbescheinigung kann als Entlastungsbeweis zu wenig sein. Die BSI-Handreichung nennt als Mindestangaben: Anbieter oder interne Stelle, Teilnehmende mit Name und Rolle, Datum, Uhrzeit und Dauer sowie Inhalte mit Bezug zu § 38 Abs. 3 BSIG. Genau deshalb muss Lernen belegbar sein – nicht als Formvoraussetzung, sondern weil ohne Beleg die Entlastung scheitert.

Was sich zuletzt bewegt hat

Die Schulungspflicht gilt seit dem 6. Dezember 2025 unmittelbar, ohne Übergangsfrist. Das BSI hat seine Handreichung zur Geschäftsleitungsschulung mehrfach aktualisiert (Fassung vom 17. April 2026). Allgemeine Nachweisanforderungen nach § 61 Abs. 3 BSIG darf das BSI frühestens am 6. Dezember 2028 stellen, bei zugelassenen Krankenhäusern frühestens am 6. Dezember 2030 – die Pflicht selbst gilt aber schon jetzt. Die KI-Kompetenz-Pflicht nach Art. 4 KI-VO ist bereits seit dem 2. Februar 2025 anwendbar.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-3

Primärquellen: § 38 Abs. 3, § 30 Abs. 2 Nr. 7, §§ 61, 62, 65 BSIG (BGBl. 2025 I Nr. 301, geändert durch BGBl. 2026 I Nr. 66) · Art. 20 Abs. 2 RL (EU) 2022/2555 · Art. 4, 113 VO (EU) 2024/1689 (EUR-Lex) · BT-Drs. 21/1501 · BSI-Handreichung „NIS-2-Geschäftsleitungsschulung“ (in der Fassung vom 17.04.2026) · § 416 ZPO

CyberPedia-Grundlage: Fachartikel „Die Schulungspflicht der Geschäftsleitung nach § 38 Abs. 3 BSIG“ (BSI-Handreichung ausgewertet mit Stand Mai 2026) und „Die zehn Mindestmaßnahmen: § 30 BSIG umsetzen“ (Stand 26.06.2026, V2.4) · Glossar: Awareness-Schulung der Mitarbeitenden, KI-Kompetenz (Art. 4 KI-VO)



Lieferketten-Durchreichung – Neue Pflichten

Was gilt

Wer als besonders wichtige oder wichtige Einrichtung unter das BSI-Gesetz fällt, schuldet nach § 30 Abs. 2 Nr. 4 BSIG die „Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern“. Die Pflicht liegt beim regulierten Kunden – nicht bei Ihnen als Zulieferer. Erfüllen kann der Kunde sie aber nur, indem er seine direkten Anbieter prüft, vertraglich bindet und laufend steuert. Genau so wandert eine Pflicht, die Sie nie unterschrieben haben, in Ihren Vertrag.

Was der Kunde dabei bewerten muss, konkretisiert Art. 21 Abs. 3 der NIS-2-Richtlinie: die spezifischen Schwachstellen seiner unmittelbaren Anbieter, die Gesamtqualität ihrer Produkte und ihrer Cybersicherheitspraxis, die Sicherheit ihrer Entwicklungsprozesse. Die Gesetzesbegründung nennt als Instrumente unter anderem vertragliche Vereinbarungen und externe Angriffsflächen-Scans. Eine einmalige Lieferantenbewertung genügt nicht – erwartet wird laufende Steuerung.

Wen es trifft

Betroffen ist der Mittelständler, der selbst nicht reguliert ist, aber regulierte Kunden beliefert: als unmittelbarer Anbieter einer NIS-2-Einrichtung, als IKT-Dienstleister eines Finanzunternehmens unter DORA – und demnächst als Hersteller, Einführer oder Händler von Produkten mit digitalen Elementen unter dem Cyber Resilience Act. Wer direkt liefert, steht vorn in der Kette.

Wo es im Buch spielt

Kapitel 10 („Lieferkette: Die offene Seitentür“ – die Lieferantenakte) und Kapitel 21 (wenn der Kunde Nachweise einkauft: Sattlers Einkaufssystem).

Der Haken

Im Finanzsektor ist die Durchreichung am härtesten: DORA verlangt vom Finanzunternehmen ein Informationsregister über alle IKT-Verträge und Mindestvertragsinhalte nach Art. 30 – bei kritischen oder wichtigen Funktionen zusätzlich umfassende Audit- und Zugangsrechte, Testmitwirkung, Untervergabe-Bedingungen und Ausstiegsstrategien. Diese Klauseln landen im Vertrag des Dienstleisters, auch wenn ihn selbst keine Aufsicht kennt; über die Untervergabe-Regeln reicht die Kette weiter bis zu seinen Subunternehmern.

Der zweite Haken: Der Kunde kann seine Pflicht nicht abgeben. Auch wenn ein Cloud-Anbieter unionsweit als kritischer IKT-Drittdienstleister überwacht wird, bleiben Register, Vertragsprüfung und Exit-Strategie Sache des Kunden – er wird also weiter fragen, prüfen und wechseln können wollen. Wer als Zulieferer Nachweise, Auditrechte und Exit-Fähigkeit nicht bieten kann, fällt schon bei der Anbieterauswahl durch.

Was sich zuletzt bewegt hat

DORA ist seit dem 17. Januar 2025 anwendbar; die Untervergabe-Regeln der Delegierten Verordnung (EU) 2025/532 sind am 22. Juli 2025 in Kraft getreten, und die BaFin sah für die Einreichung der Informationsregister 2026 ein Fenster vom 9. bis 30. März 2026 vor. Das BSI-Gesetz gilt seit dem 6. Dezember 2025, geändert durch Gesetz vom 11. März 2026. Der Cyber Resilience Act (VO (EU) 2024/2847) kommt gestaffelt: Meldepflichten für aktiv ausgenutzte Schwachstellen ab dem 11. September 2026, volle Geltung grundsätzlich ab dem 11. Dezember 2027. Der Kommissionsvorschlag COM(2026) 13 vom 20. Januar 2026 zur Änderung der NIS-2-Richtlinie ist bislang nur Monitoringpunkt.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-4

Primärquellen: § 30 Abs. 2 Nr. 4 BSIG (Stand 11.07.2026) · Art. 21 Abs. 3 RL (EU) 2022/2555 · BT-Drs. 21/1501, S. 147–149 · Art. 28, 30, 31 VO (EU) 2022/2554 (DORA) · DVO (EU) 2024/2956; DelVO (EU) 2025/532 · Art. 13, 14 VO (EU) 2024/2847 (CRA)

CyberPedia-Grundlage: Glossar „Lieferkettensicherheit (§ 30 BSIG)“, „CRA: Cyber Resilience Act“ · Fachartikel „Die zehn Mindestmaßnahmen“ (Stand 26.06.2026, V2.4), „DORA in der Tiefe“ und „DORA oder BSIG?“ (Stand 10.06.2026)



DSGVO im Cybervorfall – 72-Stunden-Meldung

Was gilt

Gemeldet wird nicht der Angriff, sondern die Verletzung des Schutzes personenbezogener Daten. Dieser Begriff ist weiter, als viele denken: Auch Vernichtung, Verlust und Veränderung von Daten zählen – eine Ransomware-Verschlüsselung ohne bewiesenen Datenabfluss kann bereits eine Verletzung sein. Die Meldung geht an die zuständige Datenschutz-Aufsichtsbehörde, nicht an das BSI. Sie erfolgt unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde – nicht ab Angriffsbeginn und nicht erst nach Abschluss der Forensik. Wer später meldet, muss die Verzögerung begründen.

Die Pflicht ist gestuft. Führt die Verletzung voraussichtlich zu keinem Risiko, entfällt die Meldung – die Dokumentation nach Art. 33 Abs. 5 DSGVO bleibt. Bei Risiko wird an die Behörde gemeldet; bei hohem Risiko werden zusätzlich die Betroffenen benachrichtigt, unverzüglich und in klarer, einfacher Sprache. Fehlende Endzahlen blockieren die Erstmeldung nicht: Art. 33 Abs. 4 trägt die schrittweise Nachmeldung. Dokumentiert wird jede bestätigte Verletzung – auch die Entscheidung, nicht zu melden.

Wen es trifft

Jeden Verantwortlichen, der personenbezogene Daten verarbeitet – unabhängig von NIS-2-Schwellen. Auftragsverarbeiter melden eine Verletzung unverzüglich an den Verantwortlichen; die Behördenmeldung bleibt grundsätzlich Sache des Verantwortlichen. Die sichere Arbeitsregel lautet: Die 72-Stunden-Frist läuft spätestens ab Eingang der Dienstleister-Meldung.

Wo es im Buch spielt

Kapitel 12 („Wenn es brennt“ – die Meldeuhren laufen parallel).

Der Haken

Der größte Denkfehler ist der Satz „Wir haben ans BSI gemeldet, also sind wir fertig.“ Die BSI-Meldung ist nicht die Datenschutzmeldung. § 32 BSIg läuft mit eigener Kaskade – Erstmeldung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussmeldung binnen eines Monats – an die gemeinsame Meldestelle von BSI und BBK. Beide Meldewege können aus demselben Cybervorfall entstehen, haben aber eigenen Auslöser, eigenen Adressaten, eigene Frist und eigenen Inhalt.

Der zweite Haken ist die Fristlogik: „Wir haben 72 Stunden Zeit“ ist die falsche Lesart – die Frist läuft ab Kenntnis, und Wochenenden sind kein Puffer. Die Verschlüsselungs-Entwarnung trägt nur, wenn die Vorkehrung auf die betroffenen Daten angewandt war und keine Schlüssel oder Klartextkopien kompromittiert sind. Verstöße gegen Melde- und Benachrichtigungspflicht sind eigenständig bußgeldbewehrt: bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes.

Was sich zuletzt bewegt hat

Das neu gefasste BSIg gilt seit dem 6. Dezember 2025; das BSI-Portal wurde zum 6. Januar 2026 als Meldestelle angekündigt. Die Verordnung (EU) 2025/2518 zur grenzüberschreitenden DSGVO-Durchsetzung ist seit dem 1. Januar 2026 in Kraft und grundsätzlich ab dem 2. April 2027 anwendbar; neue Meldepflichten schafft sie nicht. Zivilrechtlich wächst der Druck: Der EuGH hat am 4. Oktober 2024 (C-200/23) den Kontrollverlust als möglichen immateriellen Schaden anerkannt, der BGH am 18. November 2024 (VI ZR 10/24) auch den bloßen und kurzzeitigen Kontrollverlust. Auslegungsanker der Behördenpraxis bleiben die EDPB-Leitlinien 9/2022 (Version 2.0, angenommen am 28. März 2023).

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-5

Primärquellen: Art. 4 Nr. 12, 33, 34, 83 Abs. 4 lit. a DSGVO (VO (EU) 2016/679) · §§ 40, 42, 43 BDSG · §§ 32, 65 BSIG (Abruf 10.06.2026) · EDPB-Leitlinien 9/2022 V2.0 (28.03.2023) · EuGH, Urt. v. 04.10.2024 – C-200/23 (ECLI:EU:C:2024:827) · BGH, Urt. v. 18.11.2024 – VI ZR 10/24

CyberPedia-Grundlage: Fachartikel „DSGVO-Datenpanne Art. 33/34 – wann muss ich Betroffene informieren?“ (konsolidierte DSGVO-Fassung; BSIG-Prüfstand nach 06.12.2025), „BSI-Meldepflicht – die dreistufige Meldekaskade nach § 32 BSIG“ (Rechtsstand 19.06.2026, Normabrufe 10.06.2026), ergänzend „Cyber-Vorfall – die ersten 72 Stunden“



Cyber-Police – Antrag und Wirklichkeit

Was gilt

Der Antrag entscheidet mit über den Schadensfall. § 19 VVG verlangt die Anzeige der bekannten erheblichen Gefahrumstände, nach denen der Versicherer in Textform gefragt hat – vier Elemente: Frage, Kenntnis, Erheblichkeit, Zeitfenster. Wer falsch oder unvollständig antwortet, riskiert den Rücktritt; ohne Vorsatz oder grobe Fahrlässigkeit bleiben dem Versicherer Kündigung oder rückwirkende Vertragsanpassung. Bei arglistiger Täuschung kommt die Anfechtung nach § 22 VVG hinzu – dann schützt auch die gesetzliche Kausalitätsgegenprobe nicht mehr.

Nach Vertragsschluss übernehmen zwei andere Regelwerke. Wer das Risiko verändert, landet bei der Gefahrerhöhung (§§ 23 bis 27 VVG): Bei Vorsatz ist der Versicherer leistungsfrei, bei grober Fahrlässigkeit darf er nach der Schwere des Verschuldens kürzen – und die Beweislast, nicht grob fahrlässig gehandelt zu haben, trägt das Unternehmen. Vertragliche Obliegenheiten wie MFA-, Patch- oder Backup-Vorgaben laufen über § 28 VVG: Vorsatz kann leistungsfrei machen, grobe Fahrlässigkeit führt zur Quotelung. Im Schadensfall kommt die Rettungsobliegenheit des § 82 VVG dazu: Schaden abwenden, mindern, Weisungen des Versicherers befolgen.

Wen es trifft

Jede Geschäftsleitung, die einen Risikofragebogen unterschreibt oder eine Selbstauskunft freigibt. Ob die Erklärung als „Warranty“, Zusicherung oder Self-Assessment etikettiert ist, entscheidet die Rechtsfolge nicht – es zählt ihre Funktion. Und getroffen wird nicht die IT-Abteilung, sondern das Unternehmen als Versicherungsnehmer: im schlechtesten Fall ohne Deckung nach dem Cybervorfall.

Wo es im Buch spielt

Kapitel 13 („Gekauft ist nicht gedeckt“ – Antrag gegen Wirklichkeit, Obliegenheiten in den Notfallplan).

Der Haken

„Kein MFA“ bedeutet nicht automatisch Leistungsfreiheit – aber Deckung gibt es auch nicht automatisch. Jede Rechtsfolge hat Voraussetzungen: der gesonderte Hinweis in Textform (§ 19 Abs. 5 VVG), die Monatsfrist des Versicherers (§ 21 Abs. 1 VVG), bei § 28 eine wirksame Rechtsfolgenklausel und die Kausalitätsgegenprobe. Umgekehrt schützt die Gegenprobe bei Arglist nicht, und die Rechte des Versicherers reichen bei Vorsatz oder Arglist zehn Jahre zurück statt fünf.

Der stille Haken ist die Wirklichkeit hinter dem Antrag. „Wir nutzen Mehrfaktor-Authentifizierung und rollen sie auf alle privilegierten Zugänge aus“ verbindet eine Tatsache mit einer Zukunftszusage – beides wird getrennt geprüft, gegen den Ist-Zustand am Antwortzeitpunkt. Cloud-Migration, Abschalten einer Sicherheitskontrolle, neuer Dienstleister, Unternehmenskauf: alles Prüfauslöser für die Gefahrerhöhung. Wer Antrag und Betrieb nicht laufend abgleicht, führt den Beweis gegen sich selbst.

Was sich zuletzt bewegt hat

Die beiden zugrunde liegenden CyberPedia-Artikel stützen sich bewusst ausschließlich auf den Normtext – keine Aussage beruht auf einem Urteil. Bewegung kommt aus dem Gesetz: Die §§ 6 bis 9 VVG sind seit dem 19. Juni 2026 reformiert (Gesetz vom 3. Februar 2026, BGBl. 2026 I Nr. 28); eine weitere VVG-Änderung (Gesetz vom 26. Mai 2026, BGBl. 2026 I Nr. 156) tritt am 1. Januar 2027 in Kraft. Die GDV-Musterbedingungen für die Cyberrisiko-Versicherung datieren auf Februar 2024, der GDV-Muster-Risikofragebogen für KMU auf Dezember 2019 – beide ausdrücklich unverbindlich.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-6

Primärquellen: §§ 19–22, 23–27, 28, 82 VVG; §§ 119–124, 142–144, 307 BGB (Abruf 25.06.2026) · G v. 03.02.2026, BGBl. 2026 I Nr. 28; G v. 26.05.2026, BGBl. 2026 I Nr. 156 · BT-Drs. 16/3945 · GDV AVB Cyber (Februar 2024); GDV Muster-Risikofragebogen KMU (Dezember 2019)

CyberPedia-Grundlage: Fachartikel „Der Cyber-Versicherungs-Antrag: Anzeigepflicht, Underwriting und Gefahrerhöhung“ (Stand 25.06.2026, V1.3) und „Die Cyber-Police: Eigenschäden, Betriebsunterbrechung und Erpressungsdeckung“ (Stand 26.06.2026, V1.12)



D&O-Versicherung – Persönliche Haftung

Was gilt

Die D&O-Versicherung schützt nicht das Unternehmen und nicht die Server – sie schützt das private Vermögen der Geschäftsleitung, wenn diese wegen einer Pflichtverletzung persönlich in Anspruch genommen wird. Im Cybervorfall wird sie relevant, wenn der Vorwurf lautet: Die Leitung hat ihre Organisationspflichten verletzt. Forensik, Wiederaufbau und Betriebsunterbrechung sind nicht ihr Thema; das ist die Cyber-Police.

Wen es trifft

Geschäftsführer, Vorstände und Kontrollorgane wie Beiräte – persönlich, mit dem Privatvermögen. Die Gesellschaft zahlt die Prämie; geschützt ist der Mensch im Organ.

Wo es im Buch spielt

Kapitel 11 (die vierte Haftungsebene: Versicherung und persönliche Deckung) und Kapitel 13 („Gekauft ist nicht gedeckt“).

Der Haken

Fast jede D&O enthält eine Wissentlichkeitsklausel: Wer seine Pflicht kannte und trotzdem dagegen verstieß, verliert den Schutz. Genau deshalb ist der Satz „Das habe ich nicht gewusst“ vor Gericht keine Strategie, sondern ein Beweisthema.

Was sich zuletzt bewegt hat

Der Bundesgerichtshof hat im November 2025 die Position der Geschäftsleiter gestärkt: Der Versicherer muss die positive Kenntnis der konkret verletzten Pflicht nachweisen; ein bloßes „Das hätte er wissen müssen“ reicht für den Ausschluss nicht. Die Lehre daraus ist aber nicht Entwarnung, sondern das Leitmotiv dieses Buches: Ob Schutz besteht, entscheidet sich an dem, was dokumentiert ist – der rote Ordner arbeitet auch hier.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-7

Primärquellen: §§ 43–47, 100 VVG · § 93 Abs. 2 AktG; § 43 GmbHG · BGH, Urt. v. 19.11.2025 – IV ZR 66/25 (ECLI:DE:BGH:2025:191125UIVZR66.25.0); BGH, Urt. v. 18.12.2024 – IV ZR 151/23; BGH, Beschl. v. 11.02.2025 – KZR 74/23 (EuGH-Vorlage Bußgeldregress)

CyberPedia-Grundlage: Fachartikel „D&O-Versicherung im Cyber-Kontext – Wissentlichkeitsklausel und BGH IV ZR 66/25“ (Normzitate mit Abruf 04.06.2026; Gesamtausgabe Stand vom 22.07.2026)



CEO-Fraud – Der Angriff auf den Menschen

Was gilt

CEO-Fraud ist die gefälschte Chef-Anweisung zu einer Zahlung – ein Angriff auf den Menschen, nicht auf die Technik. Strafrechtlich ist das klassischer Betrug nach § 263 StGB: Ein Mitarbeiter wird getäuscht, unterliegt einem Irrtum und veranlasst eine Überweisung, die das Unternehmen schädigt. Auch Phishing, das Personen zu Zahlungen oder zur Preisgabe von Zahlungsdaten bewegt, erfüllt regelmäßig den Betrugstatbestand. Schon der Versuch ist strafbar.

Die Abgrenzung läuft über das getäuschte Gegenüber: Wird ein Mensch getäuscht, gilt § 263 StGB; wird ohne getäuschten Menschen ein Datenverarbeitungsvorgang manipuliert – etwa durch unbefugte Verwendung erbeuteter Zugangsdaten im Zahlungssystem –, greift der Computerbetrug nach § 263a StGB. Für den Cybervorfall heißt das: sauber trennen, was passiert ist – das entscheidet über Anzeige, Aufarbeitung und Versicherungsroute.

Wen es trifft

Jedes Unternehmen mit Zahlungsverkehr – vom Mittelständler bis zum Konzern. CEO-Fraud wirkt, weil er Autorität und Dringlichkeit kombiniert: Eine vermeintliche Anweisung der Geschäftsleitung setzt Mitarbeitende unter Druck, Prozesse zu überspringen. Professionelle Angriffe treffen dabei nicht nur Unaufmerksame – sie treffen jeden.

Wo es im Buch spielt

Kapitel 8 („Der Mensch öffnet die Tür“ – der neue Zahlungsprozess) und Kapitel 13 (CEO-Fraud ist nicht automatisch Cyberdeckung).

Der Haken

Technik allein fängt die menschliche Täuschung nicht ab. Was trägt, sind gehärtete Zahlungsprozesse: Vier-Augen-Prinzip und Rückrufverfahren bei Zahlungen, Multi-Faktor-Authentifizierung,

die erbeutete Passwörter entwertet, und eine Kultur, in der Nachfragen erwünscht ist – gerade bei vermeintlichen Chef-Anweisungen. Dazu gehört eine Meldekultur ohne Schuldzuweisung: Ein gemeldeter Klick ist keine Blamage, sondern Schadensbegrenzung.

Der Versicherungshaken: Die Deckung ist policeabhängig, kein Marktstandard. Social Engineering kann in einer Cyber-Police als Ausschlussfeld erscheinen; Zahlungsumleitung und sonstiger Vermögensabfluss liegen in der Deckungsdiskussion eher bei der Vertrauensschaden- oder Crime-Versicherung – beides ist ohne konkrete Bedingungsprüfung nicht belastbar. Und wer nach dem Cybervorfall Schaden oder Sicherungen gegenüber Versicherern, Banken oder Behörden bewusst falsch darstellt, riskiert selbst einen Betrug.

Was sich zuletzt bewegt hat

Die CyberPedia führt §§ 263 und 263a StGB in der geltenden Fassung mit Stand 11. Juli 2026 und dokumentiert für dieses Thema keine tragende Rechtsänderung. Der Fachartikel zu den strafrechtlichen Risiken beruht auf einer Rechtsstandprüfung vom 26. Juni 2026; der Cyber-Police-Artikel steht auf dem Stand 26. Juni 2026.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-8

Primärquellen: § 263 StGB (Betrug), § 263a StGB (Computerbetrug), geltende Fassung, Stand 11.07.2026 (gesetze-im-internet.de)

CyberPedia-Grundlage: Glossar „Betrug (§ 263 StGB)“, „Computerbetrug (§ 263a StGB)“ (Normstand 11.07.2026), „Social Engineering: den Menschen hacken“, „Phishing: Täuschung als Einfallstor“ · Fachartikel „Strafrechtliche Risiken“ (Stand 26.06.2026, V1.6), ergänzend „Die Cyber-Police“ (Stand 26.06.2026, V1.12)



EU AI Act – KI-Kompetenz und Transparenz

Was gilt

Die KI-Verordnung reguliert nach Risiko: Verbotene Praktiken (Art. 5) sind untersagt, Hochrisiko-KI (Art. 6) trägt strenge Auflagen, andere Systeme treffen vor allem Transparenzpflichten (Art. 50). Der Geltungsbeginn ist kein Stichtag, sondern ein Fahrplan nach Art. 113 KI-VO: Allgemein gilt die Verordnung seit dem 2. August 2026, die Kapitel I und II – Verbote und KI-Kompetenz – aber schon seit dem 2. Februar 2025, weitere Kapitel seit dem 2. August 2025. Maßgeblich ist stets das Kapitel, in dem die jeweilige Pflicht steht.

Der Mittelstand begegnet der Verordnung meist als Betreiber: Wer ein KI-System in eigener Verantwortung beruflich einsetzt, trägt bei Hochrisiko-KI eigene Pflichten nach Art. 26 – bestimmungsgemäße Verwendung, menschliche Aufsicht durch kompetente Personen, Überwachung des Betriebs. Unabhängig von der Risikoklasse gilt seit dem 2. Februar 2025 die KI-Kompetenzpflicht des Art. 4. Und Art. 50 verlangt Transparenz nach der Art des Systems: Chatbots müssen sich zu erkennen geben, synthetische Inhalte sind maschinenlesbar zu kennzeichnen, Deepfakes offenzulegen.

Wen es trifft

Anbieter ist, wer ein KI-System entwickelt oder entwickeln lässt und unter eigenem Namen in Verkehr bringt. Betreiber ist, wer KI in eigener Verantwortung beruflich verwendet; nur die private Nutzung ist ausgenommen. Die Rolle ist nicht statisch: Wer eine fremde Lösung unter eigenem Namen bereitstellt, kann in die Anbieterrolle rutschen. Für KMU gilt bei den Bußgeldern der jeweils niedrigere Höchstbetrag – ein Größenprivileg, das die Sanktion mildert, aber nicht aufhebt.

Wo es im Buch spielt

Kapitel 9 („KI im Giftschränk“ – die KI-Inventur, die ersten Regeln) und Kapitel 20 (die vierzig Minuten, richtig gemacht).

Der Haken

Die stufenweise Einführung darf nicht dazu verleiten, das Thema vor sich herzuschieben. Ein weiterer Irrtum ist die Hochrisiko-Einstufung als Listenabgleich: Die Rückausnahme des Art. 6 Abs. 3 verlangt eine dokumentierte Risikobewertung vor dem Inverkehrbringen.

Und die Verordnung hat scharfe Zähne: Nach Art. 99 drohen bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes für verbotene Praktiken, bis zu 15 Millionen oder 3 Prozent für sonstige Pflichtverstöße. Das Regime steht neben DSGVO und BSIG; derselbe Cybervorfall kann mehrere Regelungswelten betreffen.

Was sich zuletzt bewegt hat

Die Geltung baut sich gestuft auf: Kapitel I und II seit dem 2. Februar 2025, weitere Kapitel seit dem 2. August 2025, allgemeiner Geltungsbeginn am 2. August 2026; für Art. 6 Abs. 1 nennt die CyberPedia den 2. August 2027. Mindestens ein nationales KI-Reallabor muss nach Art. 57 seit dem 2. August 2026 einsatzbereit sein. Zu den späteren Hochrisiko-Fristen werden nach der CyberPedia Änderungen diskutiert – sie nennt dafür weder Rechtsakt noch Datum; verbindlich bleibt die jeweils geltende Fassung.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-9

Primärquellen: Art. 3, 4, 5, 6, 26, 50, 57, 99, 113 VO (EU) 2024/1689 (KI-VO), CELEX 32024R1689 (eur-lex.europa.eu/eli/reg/2024/1689/oj)

CyberPedia-Grundlage: Glossar: „KI-VO: die KI-Verordnung im Überblick“, „Geltungsbeginn der KI-Verordnung (Art. 113)“, „KI-Kompetenz (Art. 4 KI-VO)“, „Hochrisiko-KI-System (Art. 6 KI-VO)“, „KI-Anbieter“, „KI-Betreiber“, „Verbotene KI-Praktiken“, „Transparenzpflichten KI (Art. 50)“, „Bußgelder KI-Verordnung (Art. 99)“, „KI-Reallabor (Art. 57)“



Lösegeld zahlen? – Der Graubereich

Was gilt

Es gibt im deutschen Recht keine allgemeine Norm, die jede Lösegeldzahlung als solche verbietet. Daraus folgt aber nicht, dass die Zahlung unproblematisch wäre. Entscheidend sind Empfänger, Wallet, Sanktionslage, Vorsatz, Liquiditätsstatus, Versicherungsbedingungen, Meldepflichten und Dokumentation. Die Ransomware-Tat selbst ist Täterstrafrecht – Erpressung nach § 253 StGB; die Zahlung des Opfers macht das Unternehmen nicht automatisch zum Straftäter.

Das schärfste Risiko liegt häufig nicht im Strafgesetzbuch, sondern im Finanzsanktionsrecht. Das Bereitstellungsverbot bedeutet: Gelder dürfen einer gelisteten Person, Organisation oder Einrichtung weder unmittelbar noch mittelbar zugutekommen. Ein „kein Treffer“ im einfachen Namensscreening reicht nicht – geprüft werden Wallet-Adresse, Alias, Gruppenzuordnung, Eigentum und Kontrolle bis unmittelbar vor dem Transfer. Ein unklarer oder positiver Treffer bedeutet Zahlungsstopp; ein Verstoß kann nach § 18 AWG strafbar sein.

Wen es trifft

Die Geschäftsleitung jedes von Ransomware betroffenen Unternehmens – als Geschäftsleiterentscheidung unter Zeitdruck, nicht als IT-Entscheidung. Auch Nicht-Zahlen ist nicht automatisch risikoarm: Produktionsausfall, Patientensicherheit, Lieferketten und Datenveröffentlichung können existenzrelevant werden. Mitzudenken sind Verhandler, Zahlungsdienstleister, Krypto-Börsen, Versicherer und Berater mit eigenen Sanktions- und Compliance-Risiken.

Wo es im Buch spielt

Kapitel 12 (die Lösegeldfrage im Krisenstab).

Der Haken

Die Business Judgement Rule schützt nur innerhalb des rechtlich zulässigen Korridors. Sie legitimiert keinen Sanktionsverstoß, keine ausgehebelte Insolvenzordnung und keine ignorierte Meldepflicht. Nötig ist ein dokumentierter Entscheidungsvermerk: Lagebild, Alternativen, Sanktionsscreening, Strafrechtsbewertung, Insolvenzstatus, Versichererzustimmung und offene Unsicherheiten. In der Liquiditätskrise gilt zusätzlich: Eine Zahlung nach Eintritt der Insolvenzreife ist nicht einfach „Betriebsrettung“, sondern muss insolvenzrechtlich begründet werden.

Die Zahlung garantiert nichts: Der Schlüssel kann fehlen, exfiltrierte Daten können trotz Zahlung veröffentlicht werden, Nachforderungen sind möglich. Meldepflichten laufen unabhängig von der Zahlung weiter – § 32 BSIG mit der 24-Stunden-/72-Stunden-/Monatslogik, Art. 33 DSGVO mit der 72-Stunden-Frist. „Versicherung zahlt“ ist kein belastbarer Satz: Es hängt von Police, Sublimits, Sanktionsklausel und Vorab-Zustimmung ab. Das BSI rät in seiner Praxislinie grundsätzlich davon ab, auf Erpressung einzugehen – kein Rechtsverbot, aber ein wichtiger Maßstab für Alternativenprüfung und Dokumentation.

Was sich zuletzt bewegt hat

Die EU-Cyber-Sanktionen beruhen auf der Verordnung (EU) 2019/796 und dem Beschluss (GASP) 2019/797; der Stand ist dynamisch – zum CyberPedia-Stand vom 9. Juni 2026 sind insbesondere die Durchführungsverordnung (EU) 2026/1078 und der Beschluss (GASP) 2026/1079 mitzuziehen, vor jeder realen Entscheidung ist die Liste tagesaktuell zu prüfen. § 89c StGB erfasst in der 2026-Fassung auch das Sammeln, Entgegennehmen und Zurverfügungstellen von Vermögenswerten. International liegen die UK/OFSI-Ransomware-Guidance (Stand 28. Januar 2026) und das OFAC-Advisory vom 21. September 2021 vor – relevant bei entsprechendem Bezug.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-10

Primärquellen: §§ 253, 89c, 129–129b, 34 StGB; §§ 18, 19 AWG (Abruf 09.06.2026) · §§ 15a, 15b InsO; § 43 GmbHG; §§ 93, 116 AktG; §§ 32, 38 BSIG · VO (EU) 2019/796; Beschluss (GASP) 2019/797; DVO (EU) 2026/1078; Beschluss (GASP) 2026/1079 (eur-lex.europa.eu) · Art. 33 DSGVO

CyberPedia-Grundlage: Fachartikel „Lösegeld – zahlen oder nicht? Die Ransomware-Entscheidung für die Geschäftsleitung“ (Sanktionsstand und Normabrufe 09.06.2026) · Glossar „Sanktionslisten-Prüfung bei Cyber-Vorfällen“, „Erpressung (§ 253 StGB)“ (Normstand 11.07.2026)



DORA – Die Finanzkunden-Kette

Was gilt

DORA, die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor, trat am 16. Januar 2023 in Kraft und ist seit dem 17. Januar 2025 anwendbar. Direkt erfasst sind die Finanzunternehmen des Art. 2 – von Kreditinstituten über Zahlungs- und Wertpapierinstitute bis zu Versicherern; deutsche Erstreckungsfälle nach § 1a KWG und § 293 Abs. 5 VAG kommen hinzu. Der IKT-Drittdienstleister steht zwar im Geltungsbereich, ist aber gerade kein „Finanzunternehmen“. DORA ist kein allgemeines Cybersicherheitsprogramm, sondern ein aufsichtsrechtliches Betriebsmodell für den Finanzsektor.

Für Drittparteien verlangt DORA vom Finanzunternehmen laufenden Betrieb, kein Projekt: ein Informationsregister über alle IKT-Verträge (Art. 28 Abs. 3) mit mindestens jährlichem Bericht an die Aufsicht, Mindestvertragsinhalte nach Art. 30 Abs. 2 – Leistungsorte, Datenrückgabe bei Vertragsende oder Insolvenz, Vorfallunterstützung, Kündigungsrechte – und bei kritischen oder wichtigen Funktionen zusätzlich Auditrechte einschließlich Vor-Ort-Kooperation, Testmitwirkung, Untervergabe-Bedingungen und Ausstiegsstrategien (Art. 30 Abs. 3). Kritische IKT-Drittdienstleister stuft eine Europäische Aufsichtsbehörde nach Art. 31 ein und überwacht sie unionsweit.

Wen es trifft

Den nicht regulierten Mittelständler, der Software, Cloud-, Rechenzentrums- oder sonstige IKT-Leistungen an ein Finanzunternehmen liefert. Er wird nicht selbst beaufsichtigt – aber sein Vertrag wird es faktisch: Registerdaten, Art.-30-Klauseln, Auditrechte, Exit-Regeln und die Prüfung seiner Subunternehmer kommen vom Kunden. Wer Finanzkunden halten will, muss DORA-fähig liefern können.

Wo es im Buch spielt

Kapitel 16 („Sonderfälle sind selten Auswege“ – die These: Regulierung wandert über Verträge).

Der Haken

„Unser Anbieter ist beaufsichtigt, also sind wir fertig“ ist falsch – die Pflichten des Finanzunternehmens bestehen unabhängig von der unionsweiten Überwachung seines Dienstleisters weiter, und genau deshalb reicht er sie ungebremst durch. Verhältnismäßigkeit entlastet nicht: Art. 4 ist eine Anwendungsregel, der vereinfachte Rahmen nach Art. 16 kein Opt-out, sondern ein anderes Pflichtenprogramm.

Für deutsche Häuser kommt die doppelte Prüfung dazu: DORA-Status und BSIG-Einrichtungsstatus sind zwei getrennte Fragen. § 28 Abs. 6 BSIG verdrängt nur eine abschließende Liste von BSIG-Pflichten – die Registrierung nach § 33 BSIG bleibt. Und die Konzern-IT-Tochter ist nicht „mitbefreit“, nur weil die Gruppe unter DORA steht; ihr eigener BSIG-Status ist separat zu prüfen.

Was sich zuletzt bewegt hat

Das Level-2-Programm stand zum CyberPedia-Stand vom 10. Juni 2026 weitgehend: Vorfallmelde-Regeln (EU) 2025/301 und 2025/302 in Kraft seit dem 12. März 2025, Untervergabe-Regeln (EU) 2025/532 seit dem 22. Juli 2025, Testregeln (EU) 2025/1190 seit dem 8. Juli 2025. Die BaFin sah für die Einreichung der Informationsregister 2026 ein Fenster vom 9. bis 30. März 2026 vor. Der deutsche Erstreckungspfad § 1a Abs. 2a KWG gilt ab dem 1. Januar 2027.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-11

Primärquellen: VO (EU) 2022/2554 (DORA), insb. Art. 2, 4, 16, 28, 30, 31, 46 · DelVO (EU) 2024/1502, 2025/532, 2025/1190; DVO (EU) 2024/2956, 2025/301, 2025/302 · § 1a KWG; § 293 Abs. 5 VAG · § 28 Abs. 6, § 33 BSIG

CyberPedia-Grundlage: Fachartikel „DORA in der Tiefe – Pflichtenprogramm, Schulung und Aufsicht“ (Rechtsstand und Abruf 10.06.2026) und „DORA oder BSIG? – Die Abgrenzung für Finanzunternehmen“ (Stand 10.06.2026)



Nachweis – ISO 27001, BSIG, Auditfähigkeit

Was gilt

Die gesetzliche Basis ist unscheinbar und hart zugleich: § 30 Abs. 1 Satz 3 BSIG verlangt, dass die Einrichtung die Einhaltung ihrer Risikomanagementpflichten dokumentiert. Ein Dateiformat schreibt das Gesetz nicht vor; die amtliche Begründung nennt als mögliche Dokumentationen unter anderem interne Richtlinien, Checklisten, Schulungen, Auditberichte, Zertifizierungen und Prüfungen. ISO/IEC 27001 ist dabei freiwillig: Ein Zertifikat einer akkreditierten Stelle belegt ein geprüftes Managementsystem und stützt Nachweispflichten – es ersetzt aber nicht die eigenständige Erfüllung der gesetzlichen Pflichten. Normen wie ISO 27001, BSI-Grundschutz und ENISA-Leitlinien konkretisieren zugleich den Stand der Technik, einen beweglichen Maßstab.

Die proaktive Nachweispflicht des § 39 BSIG trifft dagegen nur Betreiber kritischer Anlagen: Sie müssen die Umsetzung ihrer Maßnahmen grundsätzlich alle drei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber dem BSI belegen – einschließlich der aufgedeckten Mängel. Alle anderen Einrichtungen liefern erst, wenn die Aufsicht Nachweise nach §§ 61, 62 BSIG anfordert. Daneben ist das BSI nach § 52 BSIG nationale Zertifizierungsstelle – ein Vertrauensanker für Einkauf und Lieferkette.

Wen es trifft

Die Dokumentationspflicht aus § 30 Abs. 1 Satz 3 BSIG trifft jede besonders wichtige und wichtige Einrichtung – sie ist der Normalfall, nicht die Ausnahme. Die Drei-Jahres-Nachweispflicht des § 39 BSIG gilt ausschließlich für Betreiber kritischer Anlagen. Eine ISO-27001-Zertifizierung steht jeder Organisation offen – als freiwilliger externer Nachweis gegenüber Kunden, Partnern und Aufsicht.

Wo es im Buch spielt

Kapitel 14 („Nachweis ist Substanz“ – das offene Ticket, die ehrliche Ampel) und Kapitel 21 (Nachweise als Verkaufsargument).

Der Haken

Der Kernirrtum lautet: „Wir sind zertifiziert, also sind wir compliant.“ Die CyberPedia hält dagegen: Ein Zertifikat nach einer Managementsystemnorm ersetzt nicht die einrichtungsbezogene Prüfung des gesetzlichen Schutzzumfangs, aller zehn Themenbereiche, der Verhältnismäßigkeit und der Wirksamkeit. Das Zertifikat belegt ein System, keine Unangreifbarkeit. Werben darf man nach § 52 BSIG zudem nur mit einem tatsächlich erteilten, gültigen Zertifikat.

Auch der § 39-Nachweis ist keine Formsache: Eine bloße Selbsterklärung genügt nicht, und der Nachweis endet nicht mit der Vorlage des Audits – das BSI kann die zugrunde liegende Dokumentation, einen Mängelbeseitigungsplan und den Beleg der erfolgten Behebung verlangen. Auditfähigkeit ist deshalb Führungsaufgabe: Turnus festlegen, gegen anerkannte Maßstäbe prüfen, Befunde abarbeiten, Nachweise revisionssicher ablegen – und regelmäßig gegen den aktuellen Stand der Technik fortschreiben.

Was sich zuletzt bewegt hat

Der § 39-Zyklus ist terminiert: erster Nachweis spätestens drei Jahre nach der Betreiberstellung, danach alle drei Jahre; für frühere KRITIS-Betreiber knüpft § 39 Abs. 3 BSIG an den letzten Nachweis nach altem Recht an. Auf EU-Ebene verzeichnet die CyberPedia die Änderung des EUCC-Zertifizierungsschemas durch die Verordnung (EU) 2025/2462 sowie die Kommissionsvorschläge COM(2026) 11 und COM(2026) 13 vom 20. Januar 2026 – Letztere ausdrücklich nur als Monitoringpunkte (Rechtsstand des Fachartikels: 26. Juni 2026).

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-12

Primärquellen: § 30 Abs. 1 S. 3 BSIG · § 39 BSIG (Stand 10.07.2026) · § 52 BSIG (Stand 11.07.2026) · DVO (EU) 2024/2690 · VO (EU) 2025/2462 (EUCC) · BSI-Grundschutz, ENISA-Leitlinien, ISO/IEC-27000-Reihe (laut Quellenvermerk der Glossareinträge)

CyberPedia-Grundlage: Fachartikel „Die zehn Mindestmaßnahmen: § 30 BSIG umsetzen“ (Stand 26.06.2026, V2.4) · Glossar: Nachweispflicht (§ 39 BSIG, Normstand 10.07.2026), Zertifizierung durch das BSI (§ 52 BSIG, Normstand 11.07.2026), ISO/IEC 27001, Audit in der Informationssicherheit, Stand der Technik



Beirat – Aufsichtspflicht und Haftung

Was gilt

Der Aufsichtsrat konfiguriert keine Firewall – er überwacht, ob die Geschäftsleitung die Cyber-Risiken kennt, priorisiert, finanziert, nachhält und berichtet (§ 111 AktG). Reichen die Berichte nicht, darf er nicht warten: § 111 Abs. 2 AktG gibt ihm Einsichtsrechte und das Recht, Sachverständige zu beauftragen. Haftungsanker ist § 116 in Verbindung mit § 93 AktG – mit derselben Beweislastumkehr, die auch den Vorstand trifft. Ein Cybervorfall macht den Aufsichtsrat nicht automatisch zum Schuldner; seine eigene, schuldhaft verletzte Überwachungspflicht schon.

In der GmbH gilt das über § 52 GmbHG für den gesellschaftsvertraglich bestellten Aufsichtsrat entsprechend. Beim Beirat entscheidet nicht der Name, sondern die Satzung: Ein rein beratender Familienbeirat haftet anders als ein Gremium mit Zustimmungsvorbehalten, Informationsrechten und Bestellungskompetenz. Je organähnlicher der Beirat ausgestaltet ist und gelebt wird, desto näher rückt die Organhaftung.

Wen es trifft

Aufsichtsräte der AG, gesellschaftsvertragliche und mitbestimmte GmbH-Aufsichtsräte, Genossenschafts-Aufsichtsräte und Verwaltungsräte der monistischen SE – und Beiräte, sobald sie tatsächlich überwachen statt nur zu beraten. Im Familienunternehmen ist genau diese Abgrenzung die erste Prüfung, noch vor jedem Paragraphen.

Wo es im Buch spielt

Kapitel 15 („Der Beirat auf dem Wachturm“ – Lagebild, Beiratsbericht, Zustimmungsvorbehalte).

Der Haken

Information ist Bringschuld des Vorstands – aber der Aufsichtsrat darf sie nicht passiv vermissen. Unklare, verspätete oder beschönigende Berichte lösen eine Nachfasspflicht aus; „Alles im Griff“ genügt im Haftungsprozess selten als Informationsbasis. Ein Protokoll, das nur „Cyber wurde besprochen“ sagt, entlastet niemanden.

Der zweite Haken ist der Verjährungsast: Wer Ersatzansprüche gegen den Vorstand pflichtwidrig verjähren lässt, schafft einen eigenen Sekundäranspruch gegen sich selbst (BGH II ZR 152/17). Nach ARAG/Garmenbeck muss der AG-Aufsichtsrat durchsetzbare Ansprüche der Gesellschaft grundsätzlich verfolgen – auch nach einem Cyberangriff.

Was sich zuletzt bewegt hat

Am 14. Oktober 2025 hat der BGH die Informationslinie geschärft (II ZR 78/24): Die Berichtspflichten des Vorstands bleiben auch bei geringer Geschäftstätigkeit relevant, und der Aufsichtsrat muss aktiv auf brauchbare Informationen hinwirken. Zugleich liefert das seit dem 6. Dezember 2025 geltende BSIG dem Wachturm den Gegenstand seiner Kontrolle: Die Maßnahmen nach § 30 BSIG und die Geschäftsleitungspflichten nach § 38 BSIG gehören seither in die Berichtslinie erfasster Einrichtungen. Cyber gehört damit auf die Tagesordnung – nicht als jährlicher IT-Vortrag, sondern als Kontrollpunkt mit Maßnahmenstatus, Fristen und Verantwortlichen.

Rechtsstand dieser Seite: 22. Juli 2026 (CyberPedia-Gesamtausgabe). Vertiefung, Volltexte und laufende Aktualisierung: cyber.plattes.net/chb-13

Primärquellen: §§ 90, 93, 111, 116 AktG; §§ 46 Nr. 8, 52 GmbHG; §§ 34, 41 GenG; § 39 SEAG; §§ 30, 38 BSIG · BGH, Urt. v. 14.10.2025 – II ZR 78/24 (ECLI:DE:BGH:2025:141025UIZR78.24.1); BGH, Urt. v. 18.09.2018 – II ZR 152/17; BGH, Urt. v. 21.04.1997 – II ZR 175/95 (BGHZ 135, 244, „ARAG/Garmenbeck“)

CyberPedia-Grundlage: Fachartikel „Aufsichtsrats-Haftung im Cyber-Kontext – wann das Überwachungsorgan persönlich haftet“ (jüngste zitierte Entscheidung: BGH v. 14.10.2025) · Glossar: Innenhaftung (Normstand 10.07.2026), Sorgfaltspflicht (Normstand 11.07.2026)



Anhang B | Zahlen, Fälle, Quellen

Der Cyberangriff auf die Hartmann Maschinen GmbH ist erfunden. Die folgenden Seiten im Buch beschäftigen sich hingegen mit echten Fällen, mit realen Zahlen und mit den Zukunftsprognosen von Fachleuten.

Zunächst geht es um eine Umfrage unter Führungskräften, aus der sich vier wichtige Zahlen ableiten lassen. Anschließend werfen wir den Blick auf eine Studie, aus der wir vier Thesen herausfiltern.

In den letzten beiden Teilen dieses Anhangs geht es wieder um Zahlen, die einer Geschäftsführung zur Orientierung dienen sollen: Einzelne Daten aus den Bitkom-Befragungen vermitteln eine Vorstellung davon, wie der eigene Technikstand im Unternehmen im Vergleich zum Durchschnitt dasteht. Am Ende gibt es ein paar Beispiele dafür, welchen Schaden ein Cyberangriff anrichten kann.

KPMG Global AI Pulse – Vier Zahlen zur Führungsfrage

Die Studie

KPMG International befragt seit 2026 vierteljährlich Führungskräfte zum Stand der KI-Nutzung. Die zweite Welle: 2.145 Führungskräfte aus 20 Ländern, befragt vom 28. April bis 25. Mai 2026, online.

Eines sei offen gesagt, bevor Sie die erste Zahl lesen – Sie kennen diese Ehrlichkeit aus dem Cockpit, und sie gilt auch für Quellen. Die Studie befragt Unternehmen ab fünfzig Millionen US-Dollar Umsatz; viele Leser dieses Buches führen kleinere Häuser. Sie beruht auf Selbstauskunft; gemessen wird, was Führungskräfte berichten, nicht, was Prüfer festgestellt haben. Und sie belegt Zusammenhänge, keine Ursachen. Dass ein Beratungshaus, das Governance verkauft, Governance für wichtig hält, gehört ebenfalls auf den Tisch.

Warum die Zahlen trotzdem hier stehen: Sie zeigen im Großen dieselben Muster, die dieses Buch im Mittelstand erzählt. Nicht als Beweis. Als Indiz, dass Hartmanns Weg kein Einzelfall ist.

Zahl eins: Dreimal häufiger messbarer Ertrag bei klarer Verantwortung

Organisationen mit klar definierter Verantwortung für KI-Ergebnisse berichten mehr als dreimal so häufig von etabliertem Return on Investment wie Organisationen ohne: 14 gegen 4 Prozent. Bemerkenswert ist die Zahl daneben: 75 Prozent sagen, ihr CEO trage KI als strategische Priorität – aber nur 24 Prozent können benennen, wer für KI-gestützte Entscheidungen letztverantwortlich ist.

Eigentümerschaft ist häufig. Verantwortung ist selten. Es ist derselbe Unterschied, an dem Hartmann in Kapitel 5 beinahe scheiterte: „Baumann macht das“ klingt im Alltag praktisch. Im Ernstfall klingt es dünn.

Wo es im Buch spielt: Kapitel 5, 11 und 19 – Eigentümer, Entscheidung, Datum.

Zahl zwei: Fünfmal häufiger Ertrag bei voller Transparenz der Kosten

Nur rund ein Drittel der Organisationen hat volle Sicht auf die Betriebskosten seiner KI. Wer sie hat, berichtet fünfmal häufiger von etabliertem Return on Investment als, wer sie nicht hat: 15 gegen 3 Prozent.

Das ist Carolas Doppelfrage in einer fremden Statistik: Welches Risiko reduzieren wir – welchen Wert schaffen wir? Wer die zweite Antwort nicht in Zahlen geben kann, hat meist auch die Kosten nicht in Zahlen. Sichtbarkeit schafft keinen Wert. Aber ohne Sichtbarkeit weiß niemand, wo er entsteht.

Wo es im Buch spielt: Kapitel 14, 15 und 21 – Kennzahlen, Resilienzbudget, Doppelbudget.

Zahl drei: Nur ein gutes Drittel regelt den menschlichen Eingriff

35 Prozent der Organisationen beschreiben ihre Regeln dafür, wann Menschen KI-Ergebnisse übersteuern, prüfen oder korrigieren sollen, als „sehr klar“. Zwei Drittel haben diese Klarheit nicht.

Die Regel aus Kapitel 9 – die Maschine formuliert, der Mensch verantwortlich – ist damit keine Selbstverständlichkeit. Sie ist ein Vorsprung.

Wo es im Buch spielt: Kapitel 9 und 20.

Zahl vier: Fast die Hälfte fährt KI-Vorhaben zurück

49 Prozent der Organisationen haben den Einsatz von KI-Agenten verschoben, verkleinert oder infrage gestellt, weil die erwarteten Kosten den erwarteten Nutzen zu übersteigen begannen.

Das ist keine Zahl gegen die KI. Es ist die Statistik derer, die elf Baustellen gleichzeitig eröffnet haben. Frau Webers drei Prüffragen

sind das Gegenprogramm: Wo ist der Nutzen messbar? Wo ist die Datenlage am besten? Wo ist das Risiko beherrschbar?

Wo es im Buch spielt: Kapitel 19 – die Auswahl, das Weglassen.

kpmg.com/aipulse

Stand dieser Seite: 16. Juli 2026. Vertiefung, aktuellere Befragungswellen und laufende Aktualisierung: cyber.plattes.net/chb-14

Primärquelle: KPMG International, Global AI Pulse Q2 2026, Juni 2026 (Befragung 28.04.–25.05.2026, n = 2.145) · kpmg.com/aipulse



Europe 2031 – Ein Szenario zur Führungsfrage

Das Papier

Anfang Juni 2026 erschien ein Dokument, das binnen weniger Tage in Vorstandsetagen, Ministerien und Redaktionen ankam: „Europe 2031“. Es ist keine Studie, keine politische Strategie, kein Unternehmensbericht. Es ist eine Erzählung – ein bewusst zugespitztes Szenario, das Monat für Monat beschreibt, wie Europa zwischen 2025 und 2031 den Anschluss an die Künstliche Intelligenz verliert. Nicht durch eine Katastrophe. Durch viele kleine Entscheidungen, die nicht getroffen werden.

Eines sei offen gesagt, bevor Sie weiterlesen – Sie kennen diese Ehrlichkeit aus dem Cockpit, und sie gilt auch für Szenarien: „Europe 2031“ ist keine Prognose. Die Autoren kommen aus der KI-Welt und dem Investorenumfeld; sie haben eine Position, und sie wollen Handlungsdruck erzeugen. Ein Szenario belegt nichts. Es schreibt bestehende Entwicklungen fort und fragt: Was, wenn?

Warum es trotzdem hier steht: Das Papier erzählt im Großformat dasselbe Muster, das dieses Buch im Kleinformat erzählt hat. Ein Rückstand kündigt sich nicht an. Er wird nur irgendwann sichtbar – bei Hartmann um 05:17 Uhr, bei Europa, so das Szenario, im Jahr 2031. Und in beiden Fällen begann die Krise früher. An Dienstagen.

These eins: Führungspositionen gehen nicht plötzlich verloren

Das Szenario lebt von einer Beobachtung, die sich an keiner Stelle widerlegen lässt: Technologische Führungspositionen gehen nicht über Nacht verloren, sondern durch viele kleine Entscheidungen – oder durch deren Ausbleiben. Wer Entwicklungen über Jahre unterschätzt, verliert schrittweise Handlungsspielräume, ohne dass es einen Alarm gibt.

Das ist Hartmanns zweite Lektion aus Kapitel 18, auf einen Kontinent übertragen: Ein Unternehmen muss nichts falsch machen, um zurückzufallen. Es muss nur langsamer sein als die Veränderung um es herum. Gegen den Erpresser gibt es einen Notfallplan.

Gegen das langsame Unsichtbarwerden gibt es keinen Alarm – es sei denn, die Führung baut einen.

Wo es im Buch spielt: Kapitel 1, 6 und 18 – die vierzig Sekunden am Dienstagmorgen, der falsche Trost der Unklarheit, der Anruf am Vormittag.

These zwei: Entscheidend ist die Anwendung, nicht der Modellbesitz

Die öffentliche Debatte um das Szenario dreht sich um Rechenzentren, Chips und Basismodelle. Für den Mittelstand liegt die relevante Warnung eine Ebene tiefer: Problematisch wäre nicht, dass europäische Unternehmen keine eigenen Sprachmodelle entwickeln. Problematisch wäre, wenn sie auch bei der Anwendung zurückfallen – bei der Integration in Geschäftsprozesse und der Nutzung der eigenen Datenbestände.

Die entscheidende Grenze verläuft nicht zwischen Unternehmen mit und ohne eigenes KI-Modell. Sie verläuft zwischen Unternehmen, die ihr Wissen digital nutzbar machen, und solchen, deren Wissen in unverbundenen Dateien, persönlichen Postfächern und den Köpfen einzelner Mitarbeiter verbleibt.

Das ist die Schatzkarte aus Kapitel 19 als Standortfrage: Europas Rohstoff im KI-Zeitalter sind nicht Rechenzentren, sondern hochwertige, kontextreiche, spezialisierte Daten – Wartungshistorien, Angebotsordner, Mandatsakten, Erfahrungswissen. Dieser Rohstoff liegt bereits in den Betrieben. Er ist nur, wie Baumann sagen würde, nicht gehoben. Verschüttet.

Wo es im Buch spielt: Kapitel 1, 19 und 20 – der Maschinenraum, die Schatzkarte, die vierzig Minuten mit Quellenangabe.

These drei: Der Zugang zu KI ist nicht selbstverständlich

Die härteste Passage des Szenarios beschreibt eine Welt, in der der Zugang zu den leistungsfähigsten KI-Systemen kontingentiert wird – aus sicherheits- und wirtschaftspolitischen Gründen. Ob es so kommt, ist offen. Die dahinterliegenden Fragen sind für jedes Unternehmen schon heute real: Was geschieht, wenn ein Anbieter die

Preise deutlich erhöht? Wenn ein Modell eingestellt wird? Können Daten, Abläufe und Ergebnisse zu einem anderen Anbieter übertragen werden? Wo werden die Daten verarbeitet, und darf der Anbieter sie zum Training verwenden?

Souveränität bedeutet dabei nicht vollständige Unabhängigkeit – für die meisten mittelständischen Unternehmen wäre das weder realistisch noch wirtschaftlich sinnvoll. Souveränität bedeutet: Abhängigkeiten kennen, Alternativen vorbereiten, Daten exportieren können, kritisches Wissen im Haus behalten. Ein Unternehmen kann amerikanische KI-Systeme produktiv nutzen und dennoch souverän handeln – solange es seine Handlungsfähigkeit nicht vollständig an einen einzelnen Anbieter überträgt.

Das ist wörtlich die Definition aus Kapitel 1: Souveränität ist ein Organisationszustand. Und die Prüffragen dazu stehen längst in der Lieferantenakte.

Wo es im Buch spielt: Kapitel 1, 10 und 16 – Souveränität als Organisationszustand, die Lieferantenakte, der Bitkom-Befund zur Cloud-Abhängigkeit im Anhang „Die Rechnung“.

These vier: Dieselbe KI, die produktiv macht, macht Angreifer schneller

Das Szenario beschreibt auch eine verschärfte Bedrohungslage: KI-Systeme, die Schwachstellen automatisiert finden, Angriffe skalieren, Stimmen und Identitäten täuschend echt erzeugen. Unternehmen mit schwacher Verteidigung sind besonders gefährdet.

Für dieses Buch ist das keine neue Nachricht – es ist seine Achse: Was produktiv wird, wird kritisch. Jede KI-Strategie braucht gleichzeitig eine Sicherheits-, Daten- und Notfallstrategie. Es wäre ein strategischer Fehler, Mitarbeitern leistungsfähige KI-Werkzeuge bereitzustellen, ohne Zugriffsrechte, Datenklassen, Protokollierung, Schulungen und Wiederanlauf zu regeln.

Wo es im Buch spielt: Kapitel 8 und 9 – Frau Bergers einundzwanzig Minuten, die KI-Inventur – sowie der Fall des britischen Energieversorgers im Anhang „Die Rechnung“: die erste geklonte Chef-Stimme.

Was das Szenario unterschätzt

Ein Warnruf erfüllt seinen Zweck. Übernehmen sollte man ihn trotzdem nicht unkritisch – vier Einwände gehören neben das Papier.

Erstens: Europa ist nicht nur ein Standort für Basismodelle. Seine wirtschaftliche Stärke liegt in Industrie, Maschinenbau, Chemie, Energie, Gesundheit, Finanzdienstleistungen und spezialisierten Unternehmensdienstleistungen. Der Nutzen von KI entsteht nicht nur beim Entwickler des größten Modells, sondern dort, wo KI konkrete Probleme löst – an realen Produkten, Anlagen und Prozessen.

Zweitens: Rechenkapazität allein schafft keine Wettbewerbsfähigkeit. Ohne Datenqualität, Fachkräfte, Unternehmertum und schnelle Umsetzung bleiben Rechenzentren Infrastruktur ohne Wertschöpfung.

Drittens: Nicht jede technologische Entwicklung verläuft linear. Das Szenario unterstellt sehr schnelle Fortschritte und starke geopolitische Konzentration. Möglich – aber Kosten, Energiebedarf, technische Grenzen und gesellschaftliche Widerstände können den Verlauf verändern.

Viertens: Vertrauen kann ein Wettbewerbsfaktor sein. Europäische Anbieter können gerade in sensiblen Branchen davon profitieren, dass sie Datenschutz, Nachvollziehbarkeit und rechtssichere Verarbeitung glaubwürdig gewährleisten. Aber Vertrauen darf nicht nur regulatorisches Versprechen bleiben – es muss zu marktfähigen Produkten werden. Hartmanns höchste Verlässlichkeitsstufe in Sattlers Einkaufssystem ist genau das: Vertrauen, maschinenlesbar gemacht.

Die Schlussfolgerung für die Leitungssitzung

Aus „Europe 2031“ folgt für ein mittelständisches Unternehmen nicht der Auftrag, auf ein europäisches Großprojekt oder eine politische Rettungsstrategie zu warten. Es folgt eine Doppelstrategie, und sie steht seit Kapitel 1 in diesem Buch: die leistungsfähigsten verfügbaren KI-Systeme produktiv nutzen – und zugleich die eigenen Daten, das eigene Wissen und die eigene Handlungsfähigkeit schützen.

Der europäische Mittelstand muss nicht das Rennen um das größte Sprachmodell gewinnen. Er darf nur das Rennen um die intelligente Nutzung seines eigenen Wissens nicht verlieren.

Die entscheidende Frage für 2031 lautet deshalb nicht, ob ein Unternehmen ein eigenes Basismodell besitzt. Sie lautet, ob es dann noch Herr seiner Daten, seiner Prozesse und seiner Entscheidungen ist. Es ist dieselbe Frage, die Carola an einem Sonntag über dem Braten gestellt hat: Wer kann da eigentlich alles ran?

Stand dieser Seite: 18. Juli 2026. Vertiefung, vollständige Einordnung („Der Unternehmer-Kompass“) und laufende Aktualisierung: cyber.plattes.net/chb-15



Primärquelle: „Europe 2031 – What getting AI wrong means for us“, europe2031.ai, erschienen Anfang Juni 2026 · Autoren: Daan Juijn, Stan van Baarsen, Judith Dada, Maximilian Negele, Lily Stelling, Philip Fox, Alex Petropoulos, Michiel Bakker · Rezeption u. a. ZDFheute, 12.06.2026



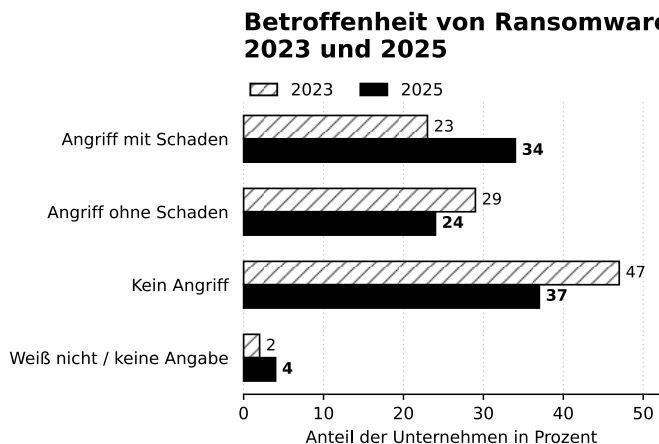
Befunde der Bitkom-Research

Als großer Think Tank treibt der Digitalverband Bitkom seit über 25 Jahren den Austausch zwischen Digitalwirtschaft, Politik, Medien Wissenschaft und Gesellschaft voran. Übergeordnetes Ziel ist es, den Standort Deutschland zu stärken und mit Forschungsergebnissen für mehr Transparenz zu sorgen.

Mit ausgesuchten Grafiken der Bitkom Research aus den Jahren 2023 bis 2026 wirft dieser Teil des Anhangs Blitzlichter auf die wachsende Bedrohungslage bei Unternehmen, auf die Herausforderungen bei der Umsetzung europäischer Richtlinien, auf das Gefühl der schwindenden Souveränität und den Altersunterschied bei der KI-Nutzung in Deutschland.

Ransomware: mehr Angriffe mit konkretem Schaden

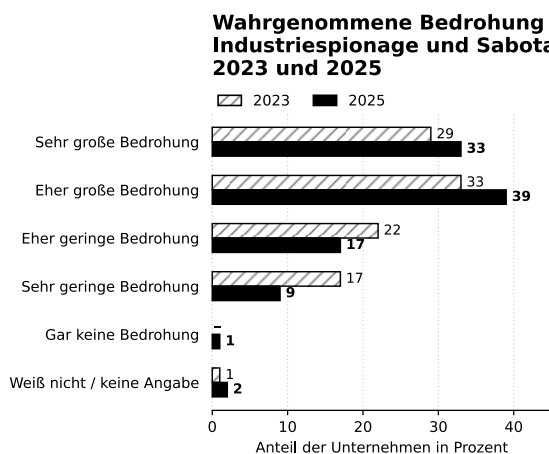
Jährlich befragt Bitkom über tausend deutsche Unternehmen mit mehr als zehn Mitarbeitern dazu, ob sie Opfer von Ransomware-Angriffen wurden. Seit Jahren liegt der Anteil der Befragten, die einen Angriff erlebt haben, bei über der Hälfte (2025: 58 Prozent). Beunruhigend ist dabei, dass die Zahl derjenigen, die den Angriff nicht abwehren konnten, sondern geschädigt wurden, von Jahr zu Jahr wächst: von 23 Prozent im Jahr 2023 auf 31 Prozent (2024) und schließlich auf 34 Prozent (2025).



Quelle: Bitkom Research. Abweichungen von 100 Prozent sind rundungsbedingt.

Datendiebstahl wird zunehmend als Bedrohung wahrgenommen

2023 sahen 62 Prozent der deutschen Unternehmen Datendiebstahl, Industriespionage und Sabotage als sehr große oder eher große Bedrohung. 39 Prozent bewerteten die Gefahr als eher gering oder sehr gering; ein Prozent machte keine Angabe.

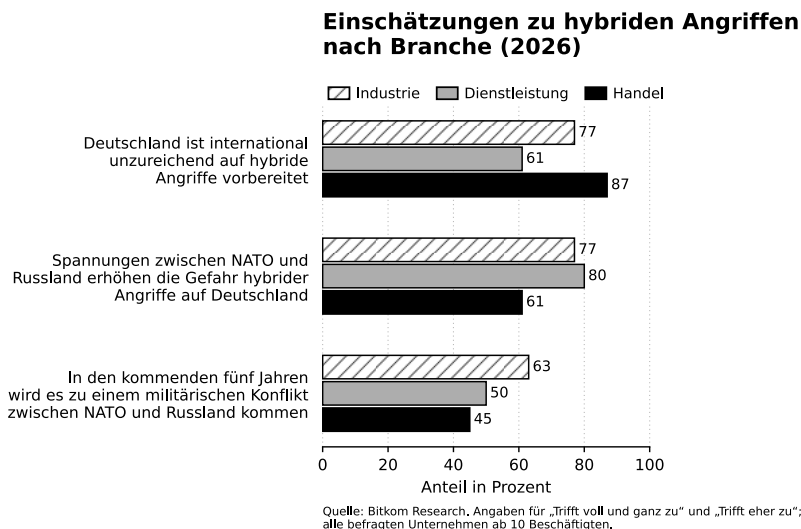


Quelle: Bitkom Research. Abweichungen von 100 Prozent sind rundungsbedingt.
Hinweis: „Gar keine Bedrohung“ wird in der 2023-Grafik nicht separat ausgewiesen.

2025 stieg der Anteil der Unternehmen mit großer Bedrohungswahrnehmung auf 72 Prozent. Gleichzeitig sank der Anteil, der die Gefahr als eher oder sehr gering einstufte, von 39 auf 26 Prozent; nur ein Prozent sah gar keine Bedrohung.

Geopolitische Spannungen verstärken die Unsicherheit

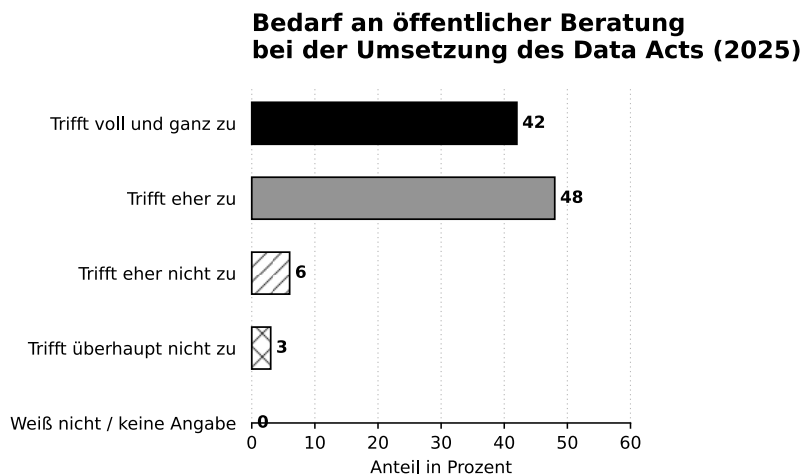
Die Gefahr, dass sich Zahl der Cyberangriffe auch durch die geopolitische Lage verstärken könnte, ist vier Jahre nach dem russischen Großangriff auf die Ukraine vielen Unternehmen bewusst.



Besonders im Handel wird die Vorbereitung Deutschlands auf hybride Angriffe kritisch gesehen: 87 Prozent halten sie für unzureichend, gegenüber 77 Prozent in der Industrie und 61 Prozent bei Dienstleistungen.

EU-Data Act: Unternehmen wünschen praktische Unterstützung

Unter den Unternehmen, die von der EU-Datenverordnung (englisch EU Data Act) betroffen sind, herrscht allgemeine Unsicherheit bei der Umsetzung. Neun von zehn Befragten wünschen sich mehr Orientierung.

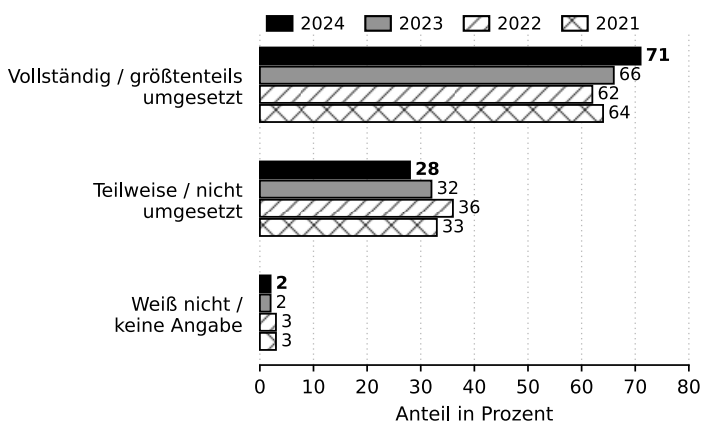


Quelle: Bitkom Research, Unternehmen, die sich vom Data Act betroffen sehen; Abweichungen von 100 Prozent sind rundungsbedingt.

DS-GVO: Fortschritt, aber keine vollständige Umsetzung

Der Anteil der Unternehmen, die die Datenschutz-Grundverordnung (DS-GVO) vollständig oder größtenteils umgesetzt sehen, stieg von 64 Prozent im Jahr 2021 auf 71 Prozent im Jahr 2024.

Stand der Umsetzung der DS-GVO 2021 bis 2024

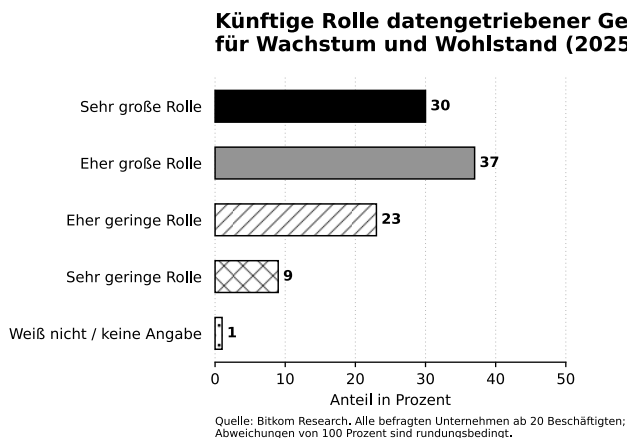


Quelle: Bitkom Research. Alle befragten Unternehmen ab 20 Beschäftigten; Abweichungen von 100 Prozent sind rundungsbedingt.

Dennoch geben 28 Prozent für 2024 an, die Vorgaben nur teilweise oder gar nicht umgesetzt zu haben – ein weiterhin erheblicher Umsetzungsrückstand.

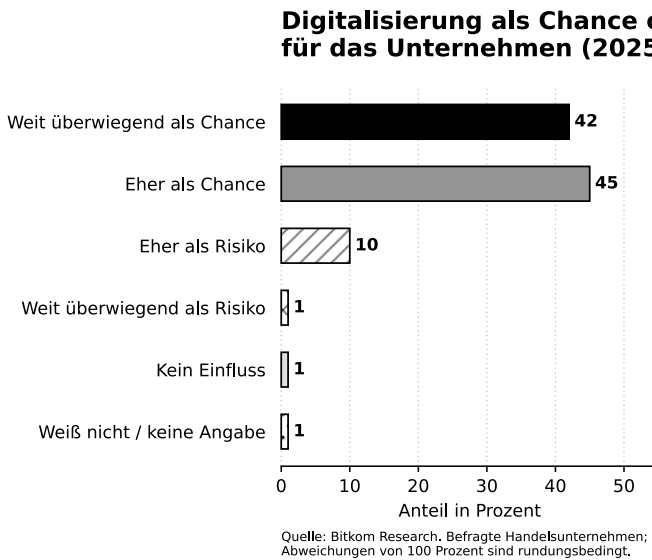
Datengetriebene Geschäftsmodelle gelten als Wachstumstreiber

67 Prozent der Unternehmen erwarten, dass datengetriebene Geschäftsmodelle künftig eine sehr große oder eher große Rolle für Wachstum und Wohlstand spielen. 32 Prozent rechnen mit einer eher oder sehr geringen Rolle; ein Prozent macht keine Angabe.



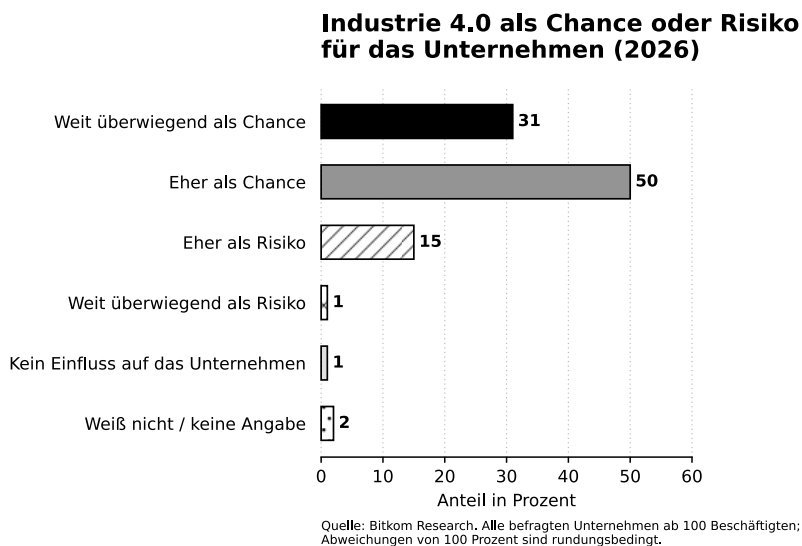
Digitalisierung wird überwiegend als Chance bewertet

2023 sahen 77 Prozent der Unternehmen die Digitalisierung weit überwiegend oder eher als Chance. 20 Prozent bewerteten sie als Risiko; die übrigen Nennungen entfielen auf keinen Einfluss oder keine Angabe.



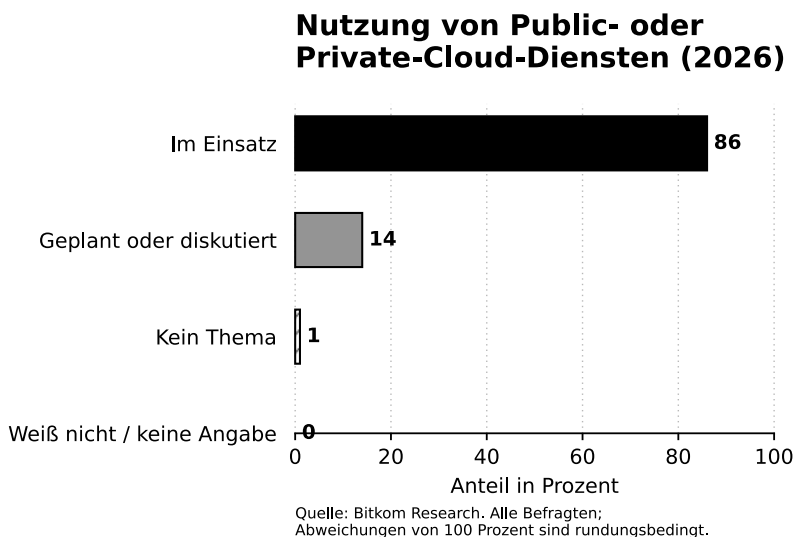
2025 stieg der Chancenanteil auf 87 Prozent, davon 42 Prozent „weit überwiegend“ und 45 Prozent „eher“ als Chance. Nur 11 Prozent sahen überwiegend ein Risiko; damit hat sich die positive Grundhaltung gegenüber 2023 deutlich verstärkt.

Auch Industrie 4.0 wird 2026 klar positiv beurteilt: 81 Prozent sehen darin weit überwiegend oder eher eine Chance. 16 Prozent verbinden sie eher oder weit überwiegend mit Risiken; drei Prozent nennen keinen Einfluss oder machen keine Angabe.

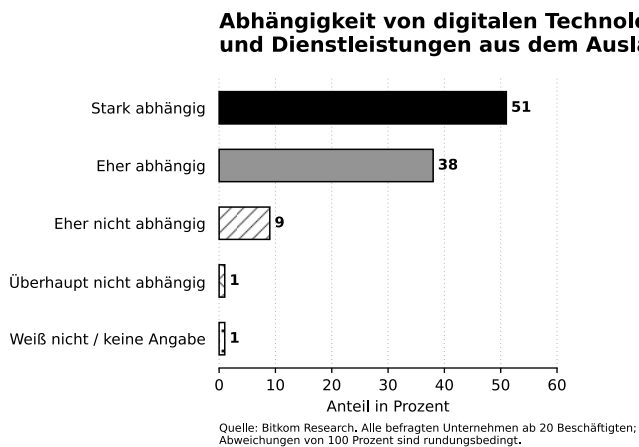


Cloud-Nutzung ist Standard – Abhängigkeit bleibt hoch

86 Prozent der Unternehmen nutzen 2026 bereits Public- oder Private-Cloud-Dienste, weitere 14 Prozent planen oder diskutieren ihren Einsatz. Cloud ist damit praktisch flächendeckend im Einsatz oder auf der Agenda.



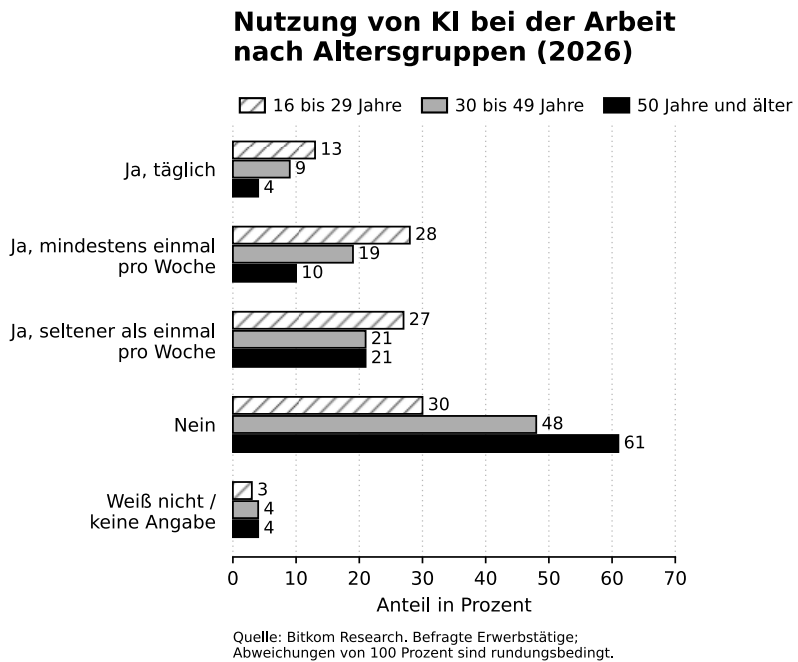
2024 stufen sich 94 Prozent der Unternehmen als „stark abhängig“ oder „eher abhängig“ vom Import beziehungsweise Bezug digitaler Technologien und Dienstleistungen aus anderen Ländern ein. Nur 4 Prozent sahen sich eher nicht oder überhaupt nicht abhängig; drei Prozent machten keine Angabe.



Im vierten Quartal 2025 lag die wahrgenommene Abhängigkeit weiterhin bei 89 Prozent, darunter 51 Prozent „stark abhängig“. Der Anteil der eher oder vollständig Unabhängigen stieg zwar auf 10 Prozent, doch die strukturelle Abhängigkeit bleibt dominant.

KI am Arbeitsplatz: deutliche Altersunterschiede

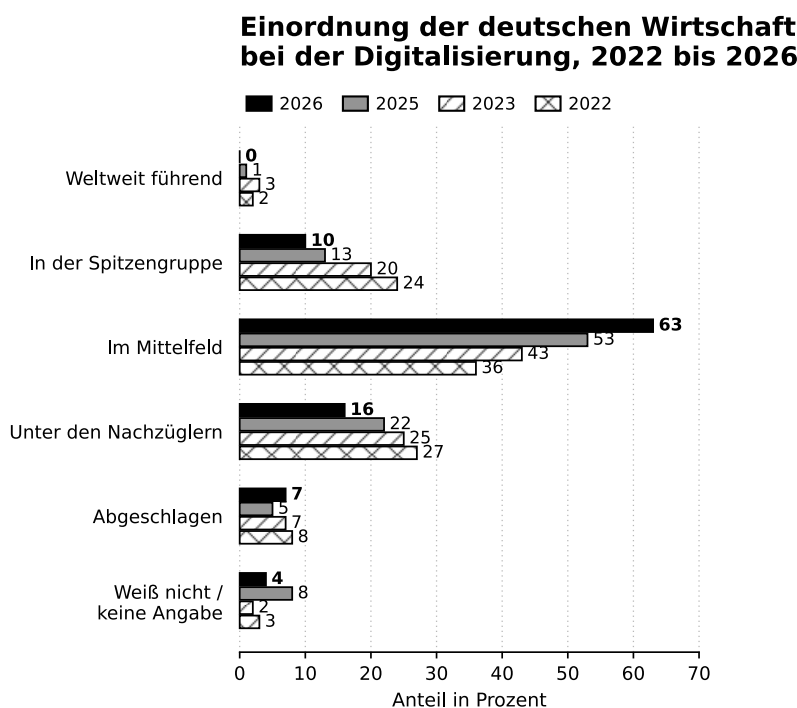
Die junge Generation wächst mit KI auf, ältere Mitarbeiter tun sich überwiegend schwer.



Bei den 16- bis 29-Jährigen nutzen 41 Prozent KI täglich oder mindestens wöchentlich; bei den 30- bis 49-Jährigen sind es 28 Prozent und bei den 50-Jährigen und Älteren 14 Prozent. Umgekehrt geben 30, 48 beziehungsweise 61 Prozent an, KI bei der Arbeit gar nicht zu verwenden.

Deutschland bleibt digital im Mittelfeld

Im Bitkom-DESI-Ranking 2025 erreicht Deutschland 50,1 Punkte und liegt damit knapp unter dem EU-Wert von 51,2. Zur Spitzengruppe um Finnland mit 77,6 Punkten besteht ein deutlicher Abstand; Deutschland befindet sich im europäischen Mittelfeld.



Quelle: Bitkom Research. Alle befragten Unternehmen ab 20 Beschäftigten; Abweichungen von 100 Prozent sind rundungsbedingt.

Auch die Selbsteinschätzung der Unternehmen fällt zurückhaltend aus: 2026 verorten 63 Prozent die deutsche Wirtschaft im weltweiten Mittelfeld, nur zehn Prozent in der Spitzengruppe und niemand als weltweit führend. Gegenüber 2022 sank der Spitzenwert von 24 auf 10 Prozent, während die Mittelfeld-Nennung von 36 auf 63 Prozent stieg.

Die Rechnung: Was Cyberangriffe kosten

Das Buch erzählt mit Thomas Hartmann eine fiktive Geschichte. Die Zahlen in diesem Anhang sind es nicht. In diesem Kapitel rückt eine Frage in den Mittelpunkt, die Unternehmer besonders interessiert: Was kostet ein Cyberangriff – und was sagen Studien über die Verwundbarkeit gerade des Mittelstands?

Die folgenden Angaben stammen aus öffentlich zugänglichen Quellen der Jahre 2025 und 2026 – darunter der Bitkom-Wirtschaftsschutz 2025, der Bitkom Cloud Report 2026, die PwC-Studie „Trügerische Sicherheit“, der IBM Cost of a Data Breach Report 2025 sowie die Lagebilder von BKA und BSI. Ergänzt werden sie um fünf reale, dokumentierte Fälle, die zeigen, wie aus abstrakten Zahlen konkrete Schäden werden.

Wichtig: Diese Zahlen sind keine Schadensprognose für ein einzelnes Unternehmen. Sie sind ein Warnsignal und eine Größenordnung. Die entscheidende Frage lautet nicht „Trifft uns genau der Durchschnitt?“, sondern „Welche unserer Prozesse, Daten und Kundenbeziehungen wären betroffen, wenn der Angriff morgen käme – und was würde uns die Wiederherstellung kosten?“

Die wichtigsten Kennzahlen auf einen Blick

Kennzahl	Wert	Quelle
Cyber als wichtigstes Geschäftsrisiko weltweit	Platz 1 · 42 %	Allianz Risk Barometer 2026
Jährlicher Gesamtschaden der deutschen Wirtschaft (Datendiebstahl, Sabotage, Spionage)	289,2 Mrd. € (+8,5 %, Rekord)	Bitkom Wirtschaftsschutz 2025
davon direkt durch Cyberangriffe	202,4 Mrd. € (≈ 70 %)	Bitkom Wirtschaftsschutz 2025
Betroffene oder vermutlich betroffene Unternehmen (Diebstahl/Spionage/Sabotage)	87 %	Bitkom Wirtschaftsschutz 2025
Ransomware-Schaden in den letzten 12 Monaten	34 % der Unternehmen	Bitkom Wirtschaftsschutz 2025
Durchschnittskosten eines Datenfalls – weltweit	4,44 Mio. USD	IBM Cost of a Data Breach 2025
Durchschnittskosten eines Datenfalls – Deutschland	3,87 Mio. €	IBM Cost of a Data Breach 2025
Digitale Erpressungsoffer, die KMU sind	90 %	BKA-Lagebild Cybercrime 2025
Mittelstand überschätzt eigene Cyber-Reife um	1–2 Reifegrade	PwC „Trügerische Sicherheit“ 2026
Unternehmen sehen sich zu stark von US-Clouds abhängig	85 %	Bitkom Cloud Report 2026

Die folgenden Abschnitte ordnen diese Zahlen ein.

Cyber ist das Geschäftsrisiko Nummer eins

Das Allianz Risk Barometer 2026 nennt Cybervorfälle zum fünften Mal in Folge als weltweit wichtigstes Unternehmensrisiko – mit 42 Prozent der Nennungen, dem höchsten je gemessenen Wert, vor

Betriebsunterbrechung, Naturkatastrophen und regulatorischen Veränderungen.

Bemerkenswert ist, wer hier antwortet: nicht IT-Abteilungen, sondern Vorstände, Geschäftsführungen, Risikomanager und Versicherer. Cyber steht also nicht auf Platz eins, weil die Technik lauter geworden ist, sondern weil die Geschäftswelt erkannt hat, dass ein Vorfall Betrieb, Reputation, Lieferfähigkeit und finanzielle Stabilität unmittelbar trifft. Cyber ist damit ein Geschäfts-, Führungs- und Vertrauensrisiko.

Der volkswirtschaftliche Schaden erreicht Rekordwerte

Die Bitkom-Studie zum Wirtschaftsschutz 2025 beziffert den jährlichen Gesamtschaden der deutschen Wirtschaft durch Datendiebstahl, Sabotage und Industriespionage auf 289,2 Milliarden Euro – ein Anstieg um rund 8,5 Prozent und der höchste je gemessene Wert. Rund 70 Prozent davon, also etwa 202,4 Milliarden Euro, gehen direkt auf Cyberangriffe zurück.

Knapp neun von zehn Unternehmen (87 Prozent) waren nach eigener Einschätzung von Diebstahl, Spionage oder Sabotage betroffen oder vermutlich betroffen. In 34 Prozent der Unternehmen hat Ransomware innerhalb der letzten zwölf Monate einen Schaden verursacht. Auffällig ist auch die Herkunft: Die Spur der Angriffe führt immer häufiger nach Russland und China.

Solche Summen sind keine exakte Rechnung für den Einzelfall. Sie zeigen aber die Größenordnung: Cyberangriffe sind kein Nischenthema der IT-Sicherheit, sondern ein volkswirtschaftliches Risiko.

Was ein einzelner Vorfall kostet

Der IBM Cost of a Data Breach Report 2025 beziffert die weltweiten Durchschnittskosten eines Datenvorfalles auf 4,44 Millionen US-Dollar (nach 4,88 Millionen im Vorjahr). Für Deutschland liegt der Durchschnitt bei 3,87 Millionen Euro – ein Rückgang gegenüber 4,9 Millionen Euro im Vorjahr, den IBM vor allem auf schnellere Erkennung durch KI-gestützte Sicherheitszentren zurückführt.

Diese Werte sind globale beziehungsweise nationale Durchschnitte und nicht eins zu eins auf jedes mittelständische Unternehmen übertragbar. Ein kleineres Unternehmen hat in der Regel geringere absolute Kosten – aber schon deutlich niedrigere Beträge können für den Mittelstand existenzbedrohend sein.

Vor allem aber steht der Schaden eines Vorfalls selten auf einer einzigen Rechnung. Er verteilt sich über Wochen und Monate auf viele Posten:

- Forensik, Wiederherstellung, neue Hard- und Software, externe IT-Dienstleister
- Betriebsunterbrechung und Produktionsausfall – oft der größte Einzelposten
- entgangener Umsatz, Vertragsstrafen, Lieferverzug
- Rechtsberatung, Datenschutzprüfung, Meldungen an Behörden
- Krisenkommunikation und Wiederaufbau von Vertrauen
- höhere Versicherungsprämien, Selbstbehalte, strengere Obliegenheiten
- Reputationsschäden, Kundenverlust, erschwerte Neukundengewinnung
- Managementzeit – ein oft unterschätzter, aber erheblicher Block

Die Kosten beginnen deshalb nicht mit der Rechnung des Forensikers. Sie beginnen mit dem Ausfall der Handlungsfähigkeit – und sie steigen mit jeder Stunde Unklarheit, mit jedem fehlenden Nachweis und mit jeder ungeübten Wiederherstellung.

Die trügerische Sicherheit des Mittelstands

Die wohl wichtigste neue Studie für dieses Buch stammt von PwC: „Trügerische Sicherheit – der Mittelstand überschätzt seine Cyber-Resilienz“ (Juni 2026), basierend auf einer Befragung von 400 Führungskräften mittelständischer Unternehmen. Ihr Kernbefund passt genau zu Hartmanns Satz „Wir sind doch kein Krankenhaus“.

Die Selbsteinschätzung der Unternehmen liegt durchgängig ein bis zwei Reifegradstufen höher als die objektiven Benchmarks, die auf

technischen Inspektionen, Dokumentenprüfungen und Interviews beruhen. Anders gesagt: Viele Mittelständler halten sich für deutlich besser geschützt, als sie es tatsächlich sind.

Diese Selbstüberschätzung spiegelt sich in den Budgets. Laut PwC investieren selbst viele größere Unternehmen weniger als 50.000 Euro pro Jahr in ihre IT-Sicherheit – für professionelles Monitoring oder getestete Notfallprozesse reicht das nicht. Der PwC-Experte Nial Moore bringt es auf den Punkt: Hier werde „am falschen Ende gespart“, denn schon das Schadenspotenzial vermeintlich kleiner Vorfälle übersteige die Kosten einer angemessenen Absicherung bei Weitem.

Weitere Befunde der Studie:

- Die Personaldecke ist dünn: Im Median arbeiten nur drei Vollzeitkräfte im Bereich Informationssicherheit.
- Rund 78 Prozent der Unternehmen setzen bereits auf externe Managed Security Services (z. B. ein Security Operations Center), um diese Lücke zu schließen.
- Nahezu die Hälfte berichtet von Cybervorfällen im eigenen Lieferantennetzwerk – aber nur jedes zweite Unternehmen kann Risiken in der Lieferkette schnell erkennen.
- Zwei Drittel der Unternehmen mit steigenden Budgets nennen KI-bezogene Risiken als Treiber – zugleich erwartet die Hälfte, dass KI die eigene Cyberabwehr massiv unterstützen wird.

Begleitet wird dieser Befund vom BKA-Lagebild Cybercrime 2025, wonach 90 Prozent der Opfer digitaler Erpressung kleine und mittlere Unternehmen sind. Der Mittelstand ist damit nicht der Zaungast der Bedrohungslage, sondern ihr Hauptschauplatz.

Ransomware und Lieferkette bleiben Haupteinfallstore

Ransomware bedeutet längst nicht mehr nur, dass Daten verschlüsselt und gegen Lösegeld freigegeben werden. Üblich ist die doppelte Erpressung: Daten werden zusätzlich kopiert, ihre Veröffentlichung wird angedroht. Der Angriff trifft dann nicht nur die

Verfügbarkeit der Systeme, sondern auch Vertraulichkeit, Datenschutz und Reputation. Ein Backup hilft gegen Verschlüsselung – nicht gegen Datenabfluss.

Parallel rückt die Lieferkette in den Fokus. PwC zufolge hat fast die Hälfte der Unternehmen bereits Vorfälle im eigenen Lieferanten-Netzwerk erlebt. Gelingt es Angreifern, Schadcode in eine verbreitete Branchensoftware einzuschleusen, erreichen sie mit einem Schlag viele Unternehmen zugleich. Gerade kleinere Betriebe sind damit doppelt interessant: Sie können selbst erpresst werden – und als Einstiegspunkt zu größeren Kunden dienen.

Künstliche Intelligenz verändert die Kostenrechnung

KI ist in diesem Buch zuerst eine Chance – sie macht eigene Daten und Prozesse produktiver. Zugleich verändert sie die Risikolage auf beiden Seiten. Angreifer nutzen KI, um Schwachstellen automatisiert zu finden und Angriffe zu skalieren; Phishing-Mails und sogar Stimmen lassen sich täuschend echt erzeugen.

Verteidiger nutzen KI ebenfalls – der Rückgang der durchschnittlichen Schadenskosten in Deutschland wird von IBM ausdrücklich auf schnellere, KI-gestützte Erkennung zurückgeführt. Entscheidend ist jedoch die Governance-Lücke: Viele Organisationen setzen KI schneller ein, als sie Richtlinien, Freigaben und Datenregeln dafür aufbauen. Genau diese Lücke zwischen KI-Nutzung und KI-Kontrolle ist für regulierte Branchen – Kanzleien, Steuerberatung, Wirtschaftsprüfung, Vermögensverwaltung, Medizin – besonders teuer, weil dort Nachweisbarkeit und Vertraulichkeit zum Produkt gehören.

Digitale Souveränität wird zum Wirtschaftsfaktor

Der Bitkom Cloud Report 2026 (Befragung von 603 Unternehmen ab 20 Beschäftigten) zeigt, wie stark das Thema Datensouveränität in der Wirtschaft angekommen ist – ein Kernmotiv dieses Buches:

- 85 Prozent der Unternehmen halten Deutschland für zu abhängig von US-Cloud-Anbietern.

- 91 Prozent würden Anbieter aus Deutschland bevorzugen – tatsächlich nutzen aber 71 Prozent US-Anbieter.
- Knapp zwei Drittel überdenken ihre Cloud-Strategie aufgrund der aktuellen US-Politik.
- 37 Prozent würden eine rein in Deutschland verarbeitende, vor fremdem Zugriff geschützte Cloud sogar mit Nachteilen wie weniger Funktionen oder höheren Kosten nutzen (nach 27 Prozent im Vorjahr).
- 90 Prozent erwarten, dass staatliche Stellen künftig stärker auf souveräne Cloud-Lösungen setzen.

Souveränität ist damit nicht nur eine politische Forderung, sondern eine betriebswirtschaftliche Erwartung: Unternehmen wollen wissen, wo ihre Daten liegen und wer darauf zugreifen kann.

Fünf reale Fälle, die die Zahlen konkret machen

Statistiken zeigen Größenordnungen. Reale Fälle zeigen, wie ein einzelner Vorfall wirkt – und welche Führungslehre er hinterlässt. Die folgenden Fälle sind öffentlich dokumentiert.

Fall (Jahr)		Schaden Summe	/ Kernlehre
FACC, Luft- & Raumfahrt (2016)		≈ 50 Mio. € ausgelöst, 41,9 Mio. € Schaden	CEO-Fraud: gefälschte Chef-Mail; CEO und CFO wurden entlassen.
Britischer (2019)	Energieversorger	220.000 € (≈ 243.000 USD)	Erster bekannter KI-Stimm-Betrug: Rückrufregeln schlagen Technik.
Colonial Pipeline, USA (2021)		4,4 Mio. USD Lösegeld (2,3 Mio. zurückgeholt)	Betriebsunterbrechung wiegt schwerer als das Lösegeld.
Equifax, USA (2017)		Vergleich bis zu 700 Mio. USD	Bekannte Lücke blieb monatelang ungepatcht – das „offene Ticket“.
Maersk / NotPetya (2017)		250–300 Mio. USD	Resilienz zählt: 4.000 Server in 10 Tagen neu aufgesetzt.

FACC (2016) – als die gefälschte Chef-Mail 50 Millionen kostete

Kriminelle gaben sich als Vorstandschef des österreichischen Luft- und Raumfahrtzulieferers FACC aus und veranlassten die Buchhaltung zu Überweisungen von rund 50 Millionen Euro für eine fiktive Übernahme. Die Bilanzbelastung lag bei 41,9 Millionen Euro; nur 10,9 Millionen Euro konnten zurückgeholt werden. Der Aufsichtsrat berief CEO und CFO ab. Der Fall zeigt: CEO-Fraud ist kein technischer Einbruch, sondern ein Angriff auf Prozesse – und er reicht bis in die Haftung der Geschäftsleitung.

Britischer Energieversorger (2019) – die geklonte Stimme des Chefs

Ein Geschäftsführer überwies 220.000 Euro, weil ihn vermeintlich der Chef der deutschen Muttergesellschaft anrief – samt vertrautem Akzent und Sprechmelodie. Die Stimme war mutmaßlich per

KI erzeugt – forensisch bewiesen wurde das nie. Es gilt als erster bekannter Fall von Stimm-Deepfake-Betrug. Die Lehre deckt sich mit Kapitel 6 des Buches: Gegen täuschend echte Kommunikation hilft kein Gehör, sondern ein Prozess – Rückruf über eine bekannte Nummer, Vier-Augen-Prinzip.

Colonial Pipeline (2021) – wenn der Betrieb teurer ist als das Lösegeld

Die Ransomware-Gruppe DarkSide legte einen der wichtigsten US-Kraftstoff-Pipelinebetreiber lahm. Das Unternehmen zahlte 75 Bitcoin (rund 4,4 Millionen US-Dollar); das FBI holte später etwa 2,3 Millionen zurück. Der eigentliche Schaden aber war die Versorgungskrise an der Ostküste. Die Lehre: Der größte Posten ist oft nicht das Lösegeld, sondern der Stillstand – und Behörden können im Ernstfall helfen.

Equifax (2017) – das teuerste offene Ticket der Geschichte

Angreifer nutzten eine bekannte Schwachstelle in einer Webanwendung, für die seit März 2017 ein Sicherheitspatch verfügbar war – eingespielt wurde er erst Ende Juli – nachdem der Einbruch bereits entdeckt war. In der Zwischenzeit wurden Daten von 147 Millionen Menschen entwendet. Der Vergleich erreichte bis zu 700 Millionen US-Dollar. Equifax ist das Lehrstück zu Kapitel 12: Ein offenes Ticket ist kein erledigtes Risiko, sondern ein Risiko mit Aktenzeichen.

Maersk / NotPetya (2017) – Resilienz als Rettung

Die Schadsoftware NotPetya traf den Logistikkonzern Maersk mit voller Wucht: 250 bis 300 Millionen US-Dollar Schaden, weltweite Betriebsunterbrechung. Bemerkenswert ist die Reaktion: Maersk setzte rund 4.000 Server, 45.000 PCs und 2.500 Anwendungen in zehn Tagen neu auf und hielt etwa 80 Prozent des Betriebs zunächst manuell aufrecht. Der Fall zeigt, was geübter Wiederanlauf und Notbetrieb wert sind – das Gegenstück zu Hartmanns „ruhigem Dienstag“.

Was die Zahlen für die Führung bedeuten

Aus diesen Zahlen folgt keine Panikpflicht, sondern eine Steuerungspflicht. Drei Befunde tragen den ganzen Anhang:

- Der Schaden ist real und groß – aber er entsteht weniger durch Technik als durch Betriebsunterbrechung, fehlende Nachweise und ungeübte Wiederherstellung.
- Der Mittelstand überschätzt sich systematisch – die gefühlte Sicherheit liegt ein bis zwei Stufen über der tatsächlichen.
- Vorsorge ist fast immer billiger als der Schaden – die teuersten Maßnahmen sind die, die man unter Zeitdruck nach dem Vorfall einkauft.

Oder als einfache betriebswirtschaftliche Faustregel: Der günstigste Euro in der Cybersicherheit ist der, der vor der Krise ausgegeben wird. Cybersicherheit ist damit Teil der Lieferfähigkeit, der Bonität, der Versicherbarkeit, der Nachfolgefähigkeit und der KIFähigkeit – kurz: Teil der Unternehmenssubstanz.

CyberPedia als digitales Nachschlagewerk

Dieses Unternehmerhandbuch ist bewusst kein Rechtskommentar und kein technisches Handbuch.

Es soll Führung ermöglichen. Es soll Unternehmer, Geschäftsführer, Vorstände, Beiräte und Unternehmerfamilien aufwecken, ohne sie in Detailrecht zu verlieren. Es erklärt, warum Cybersicherheit, KI, Datenschutz, Versicherung und Haftung zusammengehören und welche Fragen auf die Tagesordnung der Leitung gehören.

Die Vertiefung gehört in die CyberPedia.

Aufgabe der CyberPedia

Die CyberPedia ist als zweites Werk und digitales Nachschlagewerk angelegt. Sie enthält die Begriffe, Quellen, Fristen, Prüfschritte und Detailhinweise, die in Buch 1 bewusst nicht vollständig ausbreitet werden.

Dazu gehören insbesondere:

- NIS-2 und nationales Umsetzungsrecht
- BSI-Gesetz und Risikomanagementmaßnahmen
- DSGVO und Datenschutzpflichten
- EU-KI-Verordnung und KI-Governance
- DORA, KRITIS und Sonderregime
- Cyberversicherung, D&O und Obliegenheiten
- Haftungsbegriffe und Organisationspflichten
- technische Grundbegriffe wie Backup, MFA, EDR, SIEM, Zero Trust
- Vorfallmanagement, Meldekettens und Krisenkommunikation
- Glossar mit Stand, Quelle und Prüfschritt

Warum digital?

Die Rechtslage und die technische Praxis bewegen sich.

Ein gedrucktes Buch kann Orientierung geben. Ein digitales Nachschlagewerk kann gepflegt werden. Gerade bei jungen Regelwerken, sich entwickelnder Behördenpraxis und neuen KI-Anwendungen ist Aktualisierung kein Komfort, sondern Teil der Sorgfalt.

Deshalb sollte jedes Detailkapitel der CyberPedia einen klaren Stand ausweisen:

- Rechtsstand
- Quellenstand
- Prüfstatus
- Änderungsvermerk

Hinzu kommt ein Verweis auf vertiefende Beratung, wenn eine Einzelfallprüfung erforderlich ist.

Grenze der CyberPedia

Die CyberPedia ersetzt keine rechtliche Einzelfallberatung.

Sie liefert Orientierung, Struktur, Begriffe und Prüfschritte. Verbindliche rechtliche Bewertungen im konkreten Einzelfall gehören zu qualifizierten Beratern und befugten Kanzleien.

Diese Trennung ist wichtig.

Das Unternehmerhandbuch weckt und führt.

Die CyberPedia erklärt und vertieft.

Die Beratung entscheidet im Einzelfall.

Das Cockpit hält im Unternehmen nach.

Quellen

Die verwendeten Zahlen und Einordnungen beruhen auf öffentlich zugänglichen Quellen (Abruf: 30.06.2026). Für eine spätere Druckfassung sollten sie mit Titel, Herausgeber, Erscheinungsjahr, Link und Abrufdatum im Quellenverzeichnis des Buches bzw. der CyberPedia vollständig nachgewiesen werden.

1. Allianz Commercial: Allianz Risk Barometer 2026 – Cyber incidents. <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2026-cyber-incidents.html>
2. Bitkom: Wirtschaftsschutz 2025 – Lagebild der deutschen Wirtschaft (Studienbericht). https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf
3. Bitkom: Cloud Report 2026 / „Deutsche Cloud: 4 von 10 Unternehmen würden Abstriche in Kauf nehmen“ (Presseinformation). <https://www.bitkom.org/Presse/Presseinformation/Deutsche-Cloud-4-von-10-Unternehmen-wuerden-Abstriche-in-Kauf-nehmen>
4. PwC Deutschland: Studie „Trügerische Sicherheit – der Mittelstand überschätzt seine Cyber-Resilienz“, 25.06.2026 (Befragung von 400 Führungskräften); Zusammenfassung u. a. Corporate-Finance-Fachportal (Otto Schmidt). <https://cf-fachportal.de/meldungen/der-deutsche-mittelstand-ueberschaetzt-seine-cyber-abwehrkraefte/>
5. IBM: Cost of a Data Breach Report 2025. <https://www.ibm.com/reports/data-breach>
6. Bundeskriminalamt: Bundeslagebild Cybercrime 2025. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2026/Presse2026/260512_PM_BLB_Cybercrime.html
7. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2025.

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf
8. FACC AG (2016), CEO-Fraud: Berichterstattung u. a. Infosecurity Magazine. <https://www.infosecurity-magazine.com/news/ceo-sacked-after-56-million/>
 9. KI-Stimm-Betrug (2019), britischer Energieversorger: The Wall Street Journal; Zusammenfassung u. a. Forbes / Trend Micro. <https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company>
 10. Colonial Pipeline (2021): U.S. Department of Justice, „Seizes \$2.3 Million in Cryptocurrency ...“. <https://www.justice.gov/archives/opa/pr/departement-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>
 11. Equifax (2017): U.S. Federal Trade Commission, Equifax Data Breach Settlement. <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>
 12. Maersk / NotPetya (2017): Berichterstattung u. a. BleepingComputer. <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/>

Hinweis: Dieser Anhang ersetzt keine eigene Risikoanalyse und keine rechtliche Einzelfallberatung. Er liefert Größenordnungen, Studienbefunde und dokumentierte Beispiele, die zeigen, warum Cybersicherheit eine betriebswirtschaftliche Führungsaufgabe ist.

Stand dieses Anhangs: 30.06.2026.

Danksagung

Am Ende steht ein einzelner Autorenname über dem Buchtitel. Doch selbstverständlich handelt es sich bei diesem Werk um das Resultat einer gemeinsamen Anstrengung vieler schlauer Köpfe und hilfsbereiter Hände. Allen möchte ich an dieser Stelle herzlich danken. Viele bleiben anonym. Andere möchte ich namentlich erwähnen, um ihnen meine besondere Verbundenheit auszudrücken.

Christoph Ahlhaus hat nicht nur das Geleitwort geschrieben. Sein Erfahrungsreichtum ist auch in alle weiteren Kapitel eingeflossen. Kaum jemand ist so dicht am Puls der praktischen Erfahrungen der mittelständischen Unternehmen wie er. Und nur auf diese Weise konnte es gelingen, eine möglichst authentische Hartmann Maschinenbau GmbH zu erfinden.

Zu danken habe ich auch dem gesamten Team der PlattesGroup. Es ist ein gutes Gefühl, sich auf so kompetente Mitarbeiterinnen und Mitarbeiter verlassen zu können. Stellvertretend für viele bedanke ich mich bei Tom Gebhardt – für Lektorat und kritische Fragen –, bei meiner Pressechefin Claudia Schittelkopp – für ihre unermüdliche Kommunikation nach innen und außen –, bei Klaus Brandt – für die grafische Umsetzung und die Geduld bei tausend kleinen Änderungen – und bei Nils Gießler – für die technische Betreuung.

Wer mich kennt, weiß, dass ich keine Gelegenheit auslasse, meiner Frau Yvonne und unseren Kindern zu danken. Ein Familienunternehmen ist eine gemeinsame Reise, bei der es auf jeden Einzelnen ankommt. Und am Ende übertrifft das Ergebnis des Familienteams immer die Summe aller Teile.

Mein aufrichtiger Dank an alle Beteiligten.

Willi Plattes

Abkürzungen

Kürzel	Langform	Bedeutung
AI Act	Artificial Intelligence Act (EU)	EU-Verordnung über Künstliche Intelligenz („KI-Verordnung“).
AktG	Aktiengesetz	Regelt u. a. die Sorgfaltspflichten von Vorständen (§ 93).
BGH	Bundesgerichtshof	Oberstes deutsches Gericht in Zivil- und Strafsachen.
BAKA	Bundeskriminalamt	Veröffentlicht jährlich das Bundeslagebild Cybercrime.
BSI	Bundesamt für Sicherheit in der Informationstechnik	Zentrale Cybersicherheitsbehörde des Bundes.
BSIG	BSI-Gesetz	Enthält u. a. die Pflichten der Geschäftsleitung nach NIS-2 (§ 38).
CEO	Chief Executive Officer	Vorsitzende(r) der Geschäftsführung; „CEO-Fraud“: Betrug mit vorgetäuschter Chef-Identität.
CRM	Customer-Relationship-Management	Software zur Verwaltung von Kundenbeziehungen.
D&O	Directors & Officers (Versicherung)	Vermögensschaden-Haftpflicht für Organe – schützt das Privatvermögen der Leitung.
DORA	Digital Operational Resilience Act	EU-Verordnung zur digitalen Resilienz im Finanzsektor.
DSGVO	Datenschutz-Grundverordnung	EU-Regeln zum Schutz personenbezogener Daten; 72-Stunden-Meldung nach Art. 33.
ERP	Enterprise Resource Planning	Zentrale Unternehmenssoftware für Aufträge, Material, Termine und Finanzen.

Kürzel	Langform	Bedeutung
EU	Europäische Union	–
GmbHG	GmbH-Gesetz	Regelt u. a. die Sorgfaltspflichten von Geschäftsführern (§ 43).
HR	Human Resources	Personalwesen.
IP	Intellectual Property	Geistiges Eigentum (z. B. in einer IP-Gesellschaft gebündelt).
ISO	International Organization for Standardization	U. a. Norm ISO 27001 für Informationssicherheits-Management.
IT	Informationstechnik	Sammelbegriff für die technischen Systeme des Unternehmens.
KI	Künstliche Intelligenz	Systeme, die Aufgaben maschinell ausführen, für die bisher menschliche Intelligenz nötig war.
KMU	Kleine und mittlere Unternehmen	Unternehmen unterhalb der EU-Größenschwellen.
KRITIS	Kritische Infrastrukturen	Einrichtungen mit hoher Bedeutung für das Gemeinwesen (Energie, Wasser, Gesundheit u. a.).
NIS-2	Network and Information Security Directive 2	EU-Cybersicherheitsrichtlinie; in Deutschland durch das NIS-2-Umsetzungsgesetz umgesetzt.
QR	Quick Response (Code)	Maschinenlesbarer Code für Verweise auf Online-Ressourcen.
ROI	Return on Investment	Messbarer Ertrag einer Investition.
SIEM	Security Information and Event Management	System zur Sammlung und Auswertung sicherheitsrelevanter Ereignisse.

Kürzel	Langform	Bedeutung
VPN	Virtual Private Network	Dienst, der eine Internetverbindung verschlüsselt und die echte IP-Adresse verbirgt. Unternehmen stellen per VPN mitunter externen Dienstleistern einen Tunnelzugang zum IT-System zur Verfügung.
VVG	Versicherungsvertragsgesetz	Regelt u. a. Obliegenheiten und die Versicherung für fremde Rechnung.

Glossar

Dieses Glossar erklärt die zentralen Begriffe des Buches in je ein bis zwei Sätzen. Vertiefungen und laufend aktualisierte enthält das frei zugängliche Glossar der CyberPedia

cyber.plattes.net/chb-17



Backup / Wiederherstellungstest – Sicherungskopie von Daten und Systemen. Entscheidend ist nicht allein die Sicherung, sondern auch der regelmäßig geprüfte Wiederanlauf („Restore-Test“).

Betriebsunterbrechung – Zeitraum, in dem ein Unternehmen wegen eines Vorfalls nicht oder nur eingeschränkt arbeiten kann; zentraler Schadenposten der Cyber-Police.

CEO-Fraud – Betrugsmasche, bei der sich Täter als Geschäftsleitung ausgeben, um Zahlungen auszulösen – oft ganz ohne technischen Einbruch.

Cockpit – In diesem Buch: die Übersicht der Geschäftsleitung über Risiken, Maßnahmen, Nachweise und Chancen – mit ehrlicher Ampel, Verantwortlichen und Terminen.

Cyber-Police – Versicherung gegen definierte Cyberfolgen (Forensik, Wiederherstellung, Betriebsunterbrechung u. a.). Sie leistet nur im Rahmen von Bedingungen und Obliegenheiten.

D&O-Versicherung – Schützt das Privatvermögen von Geschäftsleitung und Kontrollorganen beim Vorwurf einer Pflichtverletzung – nicht das Unternehmen selbst.

Datenabfluss (Exfiltration) – Unbefugtes Kopieren von Daten aus dem Unternehmen; Grundlage der doppelten Erpressung („Zahlen, sonst veröffentlichen wir“).

Fernwartungszugang – Zugriff eines Dienstleisters von außen auf Maschinen oder Systeme; eine typische „Seitentür“, wenn er ungeprüft bleibt.

Forensik (IT-Forensik) – Fachliche Untersuchung eines Vorfalls: Wie kamen die Angreifer hinein, was haben sie getan, was ist noch kompromittiert?

Halluzination (KI) – Überzeugend formulierte, aber falsche oder erfundene Aussage eines KI-Systems.

KI-Inventur – Bestandsaufnahme aller genutzten KI-Werkzeuge: wer nutzt was, mit welchen Daten, mit welcher Freigabe und Prüfung.

Krisenstab – Festgelegte Runde, die im Ernstfall entscheidet, dokumentiert und kommuniziert – mit klaren Rollen und Vertretungen.

Mehr-Faktor-Anmeldung – Anmeldung mit einem zweiten Faktor zusätzlich zum Passwort; muss ausnahmslos für Zugänge von außen gelten.

Obliegenheit – Vertragliche Verhaltenspflicht gegenüber dem Versicherer (Meldefristen, Freigaben u. a.). Verstöße gefährden die Deckung.

Patch-Management – Geordnetes Einspielen von Sicherheitsupdates; wo das nicht möglich ist, braucht die Ausnahme Begründung, Schutzmaßnahmen und einen Plan.

Phishing – Täuschende Nachrichten, die zur Preisgabe von Daten oder zu Handlungen verleiten sollen; durch KI sprachlich kaum noch zu erkennen.

Ransomware – Schadsoftware, die Daten und Systeme verschlüsselt; die Täter fordern Lösegeld – oft verbunden mit Datenabfluss.

Resilienz – Fähigkeit, bei einem Vorfall handlungsfähig zu bleiben und geordnet wieder anzulaufen – nicht das Versprechen, dass nichts passiert.

Souveränität – Organisationszustand: wissen, welche Daten wo liegen, wer zugreift, welche Abhängigkeiten bestehen – und was im Ernstfall nachweisbar ist.

Vier-Augen-Prinzip – Kritische Vorgänge (z. B. Zahlungen ab einer bestimmten Summe) brauchen eine zweite, unabhängige Freigabe.

Stichwortverzeichnis

Dieses Register führt zu den Fundstellen in diesem Buch. Begriffserklärungen finden Sie im frei zugänglichen Glossar der CyberPedia:

cyber.plattes.net/chb-17



0

05:17 Uhr (der Anruf) 17

1

10 Fragen der
Geschäftsleitung 83

7

72 Stunden (die Zeituhr nach
einem Cybervorfall) 35,
124, 196

A

Abhängigkeit (digital) 16

AI Act (EU) 230, 282

– KI-Kompetenz-Pflicht
213

– Transparenzpflichten
230

Aktionismus 164

Angebotsassistent 172

Angebotshistorie 172

Antrag gegen Wirklichkeit
134

Auditfähigkeit 239

Auffindbarkeit (maschinell)
185

Aufsichtsbehörde 119, 219

– Anfrage 201

– Antwort 148

B

Backup siehe
Wiederherstellung

Beirat 28, 35, 150

– Beiratsbericht 122

– Wachturm 150

– Zustimmungsvorbehalte
150

Betriebsunterbrechung 55

BSI (Bundesamt für
Sicherheit in der
Informationstechnik) 33

Business Judgement Rule
207

Bußgelder 119

C

CEO-Fraud 136, 201, 227

– Versicherungsdeckung
136

– Zahlungsprozess 94

Chancen-Matrix 177

Chefsache 16

Cockpit 35, 87, 143

– Berichtsrhythmus 200

– Kennzahlen 146

– sechs Instrumente 144

Cyberangriff 47, 117, 243

– Bußgelder 119

- Innenhaftung 117
- Kosten 23
- Pflichten im Schadensfall 135
- Versicherung 34
- Cyber-Police **54**, 120, 133
 - Ausschlüsse 120
 - Obliegenheiten 55
 - Sublimits 133
- D**
- D&O-Versicherung **135**, 225
 - Wissentlichkeitsklausel 225
- Datenabfluss 83
- Datenmacht des Mittelstands 15, **21**, 33
- Datenqualität 30
- Datenschutz 19
- Deployment-Gesellschaften 21
- Dienstleister **16**, 22, 44
 - Fernwartungszugang 62
 - Lieferantenakte 112
 - Prüfung 26
- Dokumentation 26
- Domänenwissen 27
- Doppelbudget (Resilienz und Zukunft) 184
- DORA 158
- DSGVO 219, 277
 - 72-Stunden-Meldung 206
 - Information der Betroffenen 41
- E**
- Ehrliche Ampel 143
- Einkaufssystem (KI-gestützt) 30

- Erpressung, digitale siehe Ransomware
- F**
- Familienunternehmen 118
- Fernwartungszugang 62
- Forensik / Forensik-Retainer 55
- Fragebogen (Kunden-) 52
- Führungsfragen 83, 144, **193**
- G**
- Geschäftsleitung 29, 35, **83**
 - persönliche Haftung 24
 - Pflichten nach NIS-2 210
 - Schulbank der Leitung 70
- H**
- Haftung 24, 35, **117**
 - Haftungsordner 122
 - Organhaftung (§ 43 GmbHG / § 93 AktG) 207
- Halbjahresübung 163
- Halluzination (KI) 103
- Holding (kleine Gesellschaft) 77
- I**
- Incident-Log 144
- ISO 27001 239
- IT-Leiter (Rolle) 31
- J**
- Jahresreview 163
- K**
- Kennzahlen 146
- KI 16, 21, **101**

- im Giftschränk
(ungeregelte Nutzung)
101
- Inventur 58
- Kompetenz als
Führungsaufgabe 30
- quellenbasierte 27
- Richtlinie 77
- KI-Verordnung siehe AI Act
(EU)
- Krisenkommunikation 55
- Krisenstab 84
- KRITIS 16
- Kultur (schlägt Aktionismus)
57
- L**
- Lagebild, erstes 68
- Lieferantenakte 112
- Lieferfähigkeit 44
- Lieferkette 26, 35, **108**
 - als Seitentür 108
- Linie drei 26
- Lösegeldfrage 128
- M**
- Maschinenraum 23
- Maßnahmen-Matrix 89
- Mehr-Faktor-Anmeldung 52
- Meldepflichten
(Meldeuhren) 87
- Mitarbeiterinformation,
erste 126
- N**
- Nachfolge (digitale
Übergabefähigkeit) 60
- Nachweis 30, 34, **143**
 - als Substanz 147
 - maschinenlesbarer 283
 - Schulungsnachweis 122
- NIS-2 **67**, 195, 207
 - Betroffenheit (drei
Prüfungen) 73
 - Leitungspflicht 210
 - Lieferkette 108
- Notfallplan / Notfallübung
53
- O**
- Obliegenheiten 55
- Offenes Ticket 44
- Organigramm (digital) 109
- P**
- Priorisierung 66
- Produktivität 28
- Q**
- Quellenpflicht (KI-
Antworten) 27
- R**
- Ransomware 83
- Resilienz 30
- Resilienzbudget 154
- Roter Ordner 89
- Routinen, die vier 30
- Rückrufregel 57
- Rückwärtssuche 34
- S**
- Schatzkarte **174**, 191, 250
- Schulung **45**, 53, 66
 - als Rhythmus, nicht
Ereignis 134
 - der Führungskräfte 96
 - der Geschäftsleitung 83
 - der Mitarbeiter 53
 - Nachweis 143
- Sicherheitsberater, externer
47

Social Engineering 94
Souveränität 30
Störungshistorie 27
Strafrechtsschutz 120
Stresstest 33

U

Übergabefähigkeit (digital)
152
Unternehmenskultur 152

V

Verantwortung (nicht
delegierbar) 41, 61, **117**
Verbandsgeldbuße 208
Versicherung siehe Cyber-
Police; D&O-Versicherung

Vorauswahl (maschinell) 30

W

Wartungswissen 175
Weckruf 35, 141, **162**
Wiederanlauf 85
Wiederherstellung /
Wiederherstellungstest 50
Wissentlichkeitsklausel
siehe D&O-Versicherung

Z

Zahlungsprozess (Vier-
Augen- und
Rückrufprinzip) 94
Zugriffsrechte /
Zugriffsrollen 88

Nutzungshinweise und Impressum

Die Firma Hartmann Maschinenbau GmbH gibt es nicht. Aber die im Buch erzählte Geschichte liest sich auch deshalb so realistisch, weil das Unternehmen des Autors selbst zweimal zum Ziel von Cyberattacken geworden ist. Die Folgen dieser Angriffe haben die PlattesGroup lange beschäftigt und führten schließlich zu einer grundlegenden Neuaufstellung der Gruppe in Sachen Cybersicherheit und Künstlicher Intelligenz.

Ein Unternehmen, das die sich rasant ändernde Gesetzes- und Gefahrenlage nicht kennt und das keinen Überblick über Technik und notwendige Schulungen hat, ist in Gefahr. Eine Gefahr, gegen die es sich zudem nur schwer versichern kann. Denn auch der Versicherer muss für ein preislich realistisches Angebot wissen, wie hoch der Schutz, beziehungsweise wie hoch das Risiko für einen Cyberangriff ist.

Demgegenüber steht ein Unternehmen, zu dem sich die Hartmann Maschinenbau GmbH in den letzten Kapiteln des Buches entwickelt: Mitarbeiter werden regelmäßig geschult, die Lehrgänge ständig abrufbereit dokumentiert. Technische Cyberschutzlösungen können zusätzlich eingekauft und sollten idealerweise im selben Cockpit angezeigt werden. Die Unternehmensleitung behält die Übersicht und hält sich durch Fortbildungen und regelmäßige Briefings selbst auf einem aktuellen Stand. Dazu gehört selbstverständlich auch die Kenntnis darüber, welche Gesetze auf europäischer oder nationaler Ebene das eigene Unternehmen betreffen. In diesem geordneten Zustand ist es auch für einen Versicherer möglich, das – nun deutlich geringere – Restrisiko einzuschätzen und ein individuell zugeschnittenes Angebot zu machen.

Als aktuelle Nachschlagewerk über rechtliche Entwicklungen bietet die PlattesGroup zusätzlich zu diesem Buch das kostenlose Wissensportal **Willi  Pedia** an, in das sich die mehrfach erwähnte CyberPedia einordnet. Als weiteres Gratis-Angebot liefert **An:Lei-**

tung KI per Video-Podcast und Mail regelmäßige Zusammenfassungen der relevanten Entwicklungen im Bereich Cyberschutz, Künstliche Intelligenz und digitale Souveränität. Kurz und bündig. Im Stil der Memos für die Geschäftsleitung. Beide Angebote, CyberPedia und **An:Leitung KI**, sind kostenlose Bestandteile einer kommerziellen und kostenpflichtigen Dienstleistung, dem **Cyberschutzengel**.

Cyberpedia

Änderungen nach Redaktionsschluss werden im frei zugänglichen Wissensportal CyberPedia fortlaufend redaktionell aufbereitet.

cyber.plattes.net/chb-17



An:Leitung KI

Die Unternehmensleitung braucht Weitsicht. Dabei hilft An:Leitung KI mit speziellen Zusammenfassungen für den Mittelstand.

cyber.plattes.net/chb-18



Gesetzeslage, Rechtsprechung, Behördenpraxis und Versicherungsbedingungen ändern sich. Maßgeblich ist der hier und in den jeweiligen Anhangseinträgen ausgewiesene Stand; Aktualisierungen werden in der **Willi / Pedia** gepflegt und in **An:Leitung KI** besprochen. Autor und Herausgeber übernehmen keine Haftung für Entscheidungen, die allein auf Grundlage dieses Textes getroffen

werden. Das Buch ersetzt keine individuelle rechtliche, steuerliche, versicherungs- oder sicherheitstechnische Beratung. Bei Fragen mit Haftungsrelevanz sind die zuständigen Fachberater einzubinden.

Rechtsstand: August 2026.

IMPRESSUM

Willi Plattes

Zukunft mit der Datenmacht des Mittelstands

Menschen und KI-Kompetenz · Readiness · Souveränität · Resilienz

Reihe „Familienvermögen“, Band 2

1. Auflage 2026

© 2026 PlattesGroup S.L.

Camí dels Reis 308, Edificio 3A, 2º, Complejo Ca'n Granada

07010 Palma, Spain

Web: www.plattes.net

Herausgeber: PlattesGroup S.L.

Autorin: Willi Plattes

Fachredaktion: Berater, Anwälte und Fachleute der PlattesGroup

Lektorat, Satz und Layout: Tom Gebhardt, Klaus Brandt

Druck und Bindung: Amazon KDP / Druckerei

ISBN: 979-13-88469-03-9

Rechtsstand: August 2026. Dieses Fachbuch gibt die Rechtslage zum Zeitpunkt der Abfassung wieder. Steuerliche Regelungen, Steuersätze, Freibeträge sowie verwaltungs- und gerichtsrechtliche Bewertungen können sich ändern. Die Ausführungen ersetzen keine individuelle rechtliche oder steuerliche Beratung; vor jeder Entscheidung ist eine aktuelle Einzelfallprüfung erforderlich. Die dargestellten Beispiele und Beispielrechnungen dienen ausschließlich der Veranschaulichung; die genannten Personen sind frei erfunden.

Alle Rechte vorbehalten. Kein Teil dieses Werkes darf ohne schriftliche Genehmigung des Herausgebers reproduziert, unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die automatisierte Analyse dieses Werkes zur Gewinnung von Informationen über Muster, Trends und Korrelationen (Text and Data Mining gemäß § 44b UrhG) bleibt vorbehalten.

Zur Unterstützung bei stilistischen und strukturellen Überarbeitungen wurde KI eingesetzt. Die inhaltliche Verantwortung liegt vollständig bei der Redaktion.



Ihr Unternehmen ist mehr als eine Firma – es ist Ihr Lebenswerk. Es besteht aus Menschen, Kontakten, Know-how und Maschinen. Und zunehmend aus Daten und digitaler Infrastruktur. Im Zeitalter der Künstlichen Intelligenz entscheidet sich die Zukunft Ihres Unternehmens daran, wie gut Sie diesen Schatz kennen, entwickeln und nutzen.

Wer einen Schatz hebt, muss ihn schützen. Der beruhigende Satz „Wir sind doch kein Krankenhaus, wen interessieren unsere Daten?“ ist gefährlich. Diese Erkenntnis trifft Sie besser nicht erst, wenn die Bildschirme Ihrer Firma schwarz bleiben und ein Lösegeld gefordert wird. Dieses Buch zeigt, welche Auswirkungen ein Cyberangriff haben kann – und wie Sie sich Schritt für Schritt davor schützen und die Chancen der KI nutzen.

Die Wahl liegt bei Ihnen. Sie ist Chefsache.



PG
PLATTESGROUP



9 791388 469015