

# Social Engineering

Die Bedeutung des Faktors „Mensch“ in der Informationssicherheit in der Lebensmittelwirtschaft

**Teil 1:** Wie Täter durch Manipulation und Vertrauensmissbrauch Unternehmensinformationen stehlen



# Social Engineering

## Die Bedeutung des Faktors „Mensch“ in der Informationssicherheit in der Lebensmittelwirtschaft

### Teil 1: Wie Täter durch Manipulation und Vertrauensmissbrauch Unternehmensinformationen stehlen

#### Autor:innen:

- Jennifer Strunz, Social Engineer & Security Consultant
- Christian Urban, Kommunikationswissenschaftler
- Alexander Fischer, Geschäftsführer- Human Risk Consulting GmbH, Bad Wildungen  
info@hrc-gmbh.de

#### Kontakt:

DLG-Ausschuss Lebensmittelqualität und Sensorik  
Dr. Désirée Schneider (Vorsitzende)  
Bianca Schneider-Häder (Projektleiterin)  
sensorik@DLG.org

#### Disclaimer:

Die in diesem Fall beschriebenen Social Engineering Szenarien sind rein fiktiv und dienen ausschließlich informativen Zwecken. Es besteht keinerlei Absicht, irgendeine tatsächliche Person, ein Unternehmen oder eine Bäckerei zu diskreditieren, zu schädigen oder in ein negatives Licht zu rücken. Alle beschriebenen Ereignisse sind hypothetisch und fiktiv; sie sind nicht auf reale Situationen oder Akteure bezogen. Jegliche Ähnlichkeit mit tatsächlichen Personen oder Unternehmen ist rein zufällig. Der Fall soll das Bewusstsein für Sicherheitsrisiken im digitalen und physischen Umfeld schärfen und nicht dazu dienen, böswillige Handlungen zu fördern oder zu rechtfertigen.

Titelbild: © RMTH – stock.adobe.com

Alle Informationen und Hinweise ohne jede Gewähr und Haftung.

Herausgeber:

DLG e.V.  
Fachzentrum Lebensmittel  
Eschborner Landstraße 122 · 60489 Frankfurt am Main

1. Auflage, Stand 10/2024

© 2024

Alle Informationen und Hinweise ohne jede Gewähr und Haftung. Vervielfältigung und Übertragung einzelner Textabschnitte, Zeichnungen oder Bilder – auch für den Zweck der Unterrichtsgestaltung – nur nach vorheriger Genehmigung durch DLG e.V., Marketing, Eschborner Landstraße 122, 60489 Frankfurt am Main.

Immer häufiger tritt sowohl im privaten als auch im beruflichen Lebensbereich das Phänomen des „Social Engineering“ in Erscheinung. Dabei versuchen „kriminelle, skrupellose Energien“, über die gezielte Manipulation und Beeinflussung von menschlichem Verhalten gesetzeswidrige Handlungen umzusetzen. Dies können Telefon- oder Türgespräche von fiktiven Verwandten oder Bankangestellten sein, die die Freigabe von Finanzmitteln und Wertsachen fordern oder digitale „Ansprachen“ zur Preisgabe von vertraulichen Informationen.

Im nachfolgenden aus zwei Teilen bestehenden Expertenwissen, soll das Thema „Social Engineering“ näher beleuchtet und anhand fiktiver Fallbeispiele aus der Lebensmittel-Praxis den Lesern nähergebracht werden. Hilfreiche Tipps sowohl für die Personalschulung als auch für ggf. seitens der Betriebe zu treffende Vorbeugemaßnahmen runden die Publikation ab.

Im Teil 1 steht das Verhalten der Täter im Vordergrund, während im Teil 2 die Angriffsmethoden und die Maßnahmen zur Abwehr thematisiert werden.

### Teil 1: Wie Täter durch Manipulation und Vertrauensmissbrauch Unternehmensinformationen stehlen

Im Bereich der IT-Sicherheit wird häufig der Fokus auf digitale Bedrohungen wie Malware oder Hackerangriffe gelegt. Dabei wird oft übersehen, dass auch die physische Sicherheit eine entscheidende Rolle spielt. Gerade physische Sicherheitsmaßnahmen sind essenziell, um unbefugten Zugriff auf Hardware oder Netzwerke zu verhindern. Bei Versäumnis der richtigen Maßnahmen kann es zu folgenschweren Konsequenzen kommen. Angreifer sind bei vernachlässigter Sicherheit bemächtigt, Zugangskontrollen zu umgehen, Geräte zu manipulieren oder sensible Daten zu stehlen.

Um eine umfassende IT-Sicherheitsstrategie zu entwickeln, sollte gerade in der breiten Palette an Maßnahmen die physische Sicherheit nicht zu kurz kommen.



## Fallbeispiel

Ein weißes, kleines Auto parkt vor einer Bäckerei. Es ist ein unscheinbarer Mittwochmorgen und die Sonne scheint warm auf das Pflaster. Kai Wolfhardt wartet noch einige Sekunden in seinem Wagen, atmet tief durch, während er mit den Fingern auf das Lenkrad trommelt, greift dann nach seinem schwarzen Koffer, der auf dem Beifahrersitz ruht, und steigt aus. Ruhig läuft er Richtung Eingang – hinter seinem freundlich aufgesetzten Lächeln verbirgt sich jedoch eine ganz andere Absicht.

Innen herrscht geschäftiges Treiben. Mitarbeiter in weißen Schürzen und Haarnetzen stehen hinter dem Tresen, kneten Teig oder überwachen die Öfen. Eine junge Verkäuferin blickt auf, als Kai Wolfhardt durch die Tür kommt. Als sie den schwarzen Koffer erblickt, weiten sich ihre Augen. „Guten Morgen“, sagt Herr Wolfhardt mit fester Stimme. „Ich bin Kai Wolfhardt von der Lebensmittelaufsicht. Ich komme zur unangemeldeten Kontrolle.“

Die Empfangsdame wirkt sichtlich nervös und nickt eifrig. „Guten Morgen, Herr Wolfhardt. Bitte entschuldigen Sie, ich muss das fragen, aber können Sie sich ausweisen?“

„Natürlich.“ Der Kontrolleur greift in seine Hosentasche ins Leere und schnaubt. „Mein Ausweis ist im Auto. Den reiche ich aber nach Abschluss meiner Kontrolle selbstverständlich nach.“

„Alles klar“, sagt sie schnell und kramt ein paar Sachen zusammen. „Ich notiere einfach, dass Sie da waren.“

„Das brauchen Sie gar nicht. Der Geschäftsführer erhält im Laufe des Tages sowieso eine Auftragsbestätigung von mir“, entgegnet Kai ruhig. „Was unsere Geschäftsführung angeht, der ist heute leider außer Hause, aber ich kann Ihnen gerne alles zeigen. Ich bin Erika.“ „Vielen Dank, Erika. Dann fangen wir am besten gleich an.“

Nachdem Kai sich die Hygienekleidung übergezogen hat, führt Erika ihn in die Backstube. Der Geruch von Hefe und frisch gebackenem Brot ist hier noch intensiver. Die Angestellten werfen neugierige Blicke auf den Kontrolleur, setzen ihre Arbeit jedoch sichtlich nervöser fort.

„Das hier ist unsere Backstube“, erklärt Erika, während sie Kai durch die Räume führt. „Wir legen großen Wert auf Sauberkeit und Qualität“, betont sie noch.

Kai nickt und öffnet seinen Koffer. „Das freut mich zu hören. Schauen wir uns das mal genauer an.“

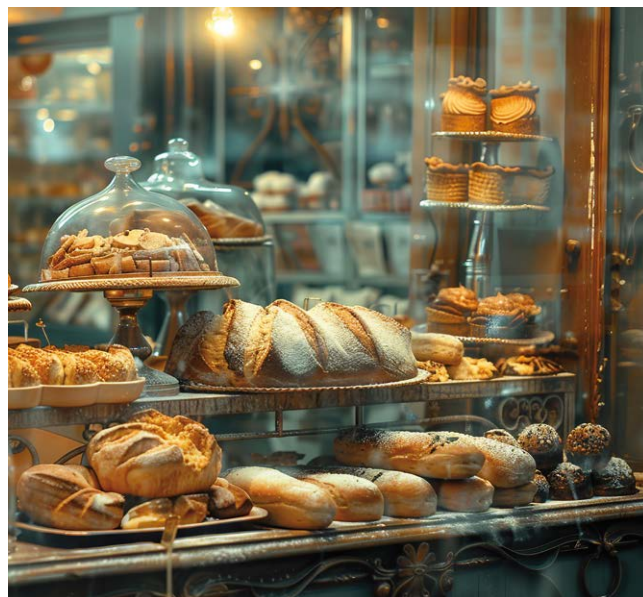
Er beginnt, Proben von verschiedenen Zutaten zu nehmen, die Sauberkeit der Arbeitsflächen zu prüfen und die Temperaturen der Kühlschränke zu messen. Während er seine Aufgaben erledigt, stellt er Erika Fragen über die Arbeitsverläufe, die sie geduldig beantwortet. Während die Mitarbeiterin über die verschiedenen Arbeitsphasen am Tag berichtet, holt Kai sein Handy aus der Hosentasche und beginnt Fotos zu machen. Vor allem Türen und Flure scheinen seine volle Aufmerksamkeit zu haben. Erika wird nervöser: „Also Fotos sind hier eigentlich nicht erlaubt...“

Kai lächelt sie warm an. „Das sind neue Vorschriften. Wir müssen Bilder machen, damit die Inspektion nachvollziehbarer wird. Das ist mein Diensthandy, die Bilder tauchen nur noch im Report auf.“

„Verstehe“, erwidert die Mitarbeiterin, die Unsicherheit nicht gänzlich verfolgen.

Während er scheinbar gewissenhaft seiner Arbeit nachgeht, lässt Kai immer wieder seinen Blick durch den Raum schweifen. Er bemerkt das kleine Büro in der Ecke und eine angelehnte Tür, die vermutlich ins Lager führt. Als Erika kurz abgelenkt ist, weil eine Kollegin die beiden begrüßt, fotografiert Kai das Büro und die offenstehende Tür. Als sie weitergehen, wirft Kai einen kurzen Blick durch den Spalt der angelehnten Tür und bemerkt am anderen Ende der kleinen Lagerhalle ein Rolltor. Dieses steht ungefähr 20-30 Zentimeter vom Boden entfernt offen, sodass Licht in die Halle drang. Das bleibt nicht unbemerkt.

Nach einer Weile kommen sie zu einem großen Metallregal mit aufgereihten Teiglingen. Kai beugt sich leicht vor und inspiziert die Teiglinge sorgfältig. „Sind diese für morgen vorgesehen?“, fragt er und deutet auf die abgedeckten Bleche.



© Stas – stock.adobe.com

„Ja, genau“, bestätigt Erika eifrig. „Wir bereiten sie immer am Vorabend vor.“ „Gut“, sagt Kai schnell und notiert sich etwas in seine Notizen.

Nach weiteren Untersuchungen und Notizen dreht sich Kai zu Erika und lächelt leicht. „Alles in allem sieht es hier sehr gut aus. Es gibt ein paar kleine Dinge, die wir verbessern können, aber insgesamt bin ich zufrieden.“

Erika atmet erleichtert auf. „Das freut mich zu hören.“

„Eine Bitte hätte ich aber noch“, beginnt er und Erika blinzelt ihn mit zusammengebißenen Zähnen an.

„Könnte ich schnell auf die Toilette? Mein nächster Termin ist eine Weile von hier entfernt.“

Erikas Kiefermuskel entspannen sich sichtlich. „Klar, natürlich. Gehen Sie einfach den Flur entlang und dann links.“

Kai nickt und verschwindet eilig mit seinem Arbeitskoffer.

Als er wieder kommt, arbeitet Erika wieder am Tresen.

Der Kontrolleur winkt ihr zu: „Ich werde Ihnen meinen Bericht in den nächsten Tagen zukommen lassen. Vielen Dank für Ihre Kooperation.“

Als Kai Wolfhardt die Bäckerei verlässt und zu seinem Wagen zurückgeht, holt er erneut sein Handy heraus und tippt eine kurze Nachricht: „Hab alle Informationen. Der Zugang zum Lager erfolgt durch die Tür neben dem Büro. Hab' keine weiteren Sicherheitsvorkehrungen gesehen...“

### Was genau ist passiert?

Auch wenn die Situation nun klar – jedenfalls nach der Auflösung, dass böse Absichten im Raum stehen – zu deuten ist, steckt so viel mehr dahinter als auf dem Blick erkennbar.

Dass Kai Wolfhardt hier definitiv kein Kontrolleur einer Lebensmittelaufsicht ist, wissen wir bereits, aber wer ist er dann? Einfach ausgedrückt: Ein Angreifer.

Aber ein Angreifer kann auch jemand sein, der mit einer Waffe in den Laden stürzt und „her mit dem Geld!“ brüllt.

Kai Wolfhardt ging strategisch vor. Er war ruhig und ließ sich kaum etwas anmerken.

In diesem Fall nennen wir das einen Social Engineering Angriff. Wie das Verfahren schon verrät, handelt es sich bei Kai um einen Social Engineer.

### Analyse der Situation

Der Social Engineer hatte sich als Lebensmittelkontrolleur ausgegeben, was in diesem Falle eine autoritative und authentische Rolle ist, die es ihm ermöglicht, Zugang zu normalerweise geschützten Bereichen zu erhalten. Um seine Rolle glaubwürdig zu spielen, hat er vermutlich schon im Voraus recherchiert, welche Ausrüstung er benötigt. Durch das selbstsichere Auftreten und entsprechender Kleidung konnte der Angreifer sofort das Vertrauen und die Kooperation der Angestellten (nicht nur die der jungen Verkäuferin) gewinnen. Das Vertrauen ging sogar so weit, dass es für Kai ausreichte, nur zu erwähnen, dass er einen Ausweis habe, den er später nachreichen möchte.

Die Abwesenheit des Geschäftsführers war entweder ein Glücksfall oder von vornherein geplant. Ohne diese direkte Aufsicht war die junge Verkäuferin Erika die Hauptkontaktperson. Erika war bemüht, entgegenzukommen, und wollte vermutlich einen guten Eindruck hinterlassen, was der Social Engineer sofort ausnutzte.

Während Kai scheinbar routinemäßige Kontrollen durchführte, beobachtete der Angreifer seine Umgebung ganz genau. Er bemerkte wichtige Details wie das kleine Büro oder die nicht verschlossene Tür zum Lager. Besser noch: Das Rolltor stand ein wenig offen und weit und breit keine Aufsicht. Solche Beobachtungen sind wertvoll für zukünftige Einbrüche und Informationsdiebstahl, da diese kritischen Sicherheitslücken mögliche Zugangspunkte liefern.

Ein weiterer Aspekt sind die gezielten Fragen, um spezifische Informationen zu den Arbeitsabläufen und der Lagerung zu erhalten. Diese sind insoweit wichtig, weil sie dem Angreifer ein besseres Verständnis der Sicherheit und Schwachstellen der Bäckerei geben. Außerdem macht sich Kai unauffällig Notizen und Bilder, um kein wichtiges Detail zu vergessen. In seiner letzten Angriffsphase fragt Kai nach der Toilette – ein unscheinbarer Trick, um unbeobachtet nochmal durch die Räumlichkeiten zu gehen.

Am Ende verabschiedete sich der Social Engineer höflich und professionell, um keinen Verdacht zu erregen. Er hinterließ sogar einen positiven Eindruck. Seine Authentizität wird zu diesem Zeitpunkt nicht angezweifelt.

## Definition: Social Engineering

Auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird „Social Engineering“ folgendermaßen definiert:

*„Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyber-Kriminelle verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.*

*Social Engineering ist an sich nichts Neues und dient seit Menschengedenken als Grundlage für die unterschiedlichsten Betrugsmaschen. Im Zeitalter der digitalen Kommunikation ergeben sich jedoch äußerst effektive, neue Möglichkeiten für Kriminelle, mit denen sie Millionen von potenziellen Opfern erreichen können.“<sup>1</sup>*

Es muss jedoch noch einmal betont werden, welche Gefahr davon ausgeht: Social Engineers sind Meister der Manipulation, die das menschliche Vertrauen als ihre stärkste Waffe einsetzen. Sie ziehen die Fäden so, dass sie ihre Opfer dazu bringen, vertrauliche Informationen preiszugeben oder ihnen helfen, Sicherheitsbarrieren zu überwinden. Oft agieren sie im Verborgenen, verkleiden sich als vertrauenswürdige Autoritätspersonen wie IT-Spezialisten oder Inspektoren (wie in der Einleitung zu lesen) und nutzen geschickt psychologische Tricks, um ihren Zielen näherzukommen. Ihr Können liegt nicht unbedingt in technischen Hacks, sondern darin, menschliche Schwächen auszunutzen, sei es durch Charme, Drohungen oder Täuschungen. Zugegeben, es klingt äußerst überhöht, aber ein Social Engineer kann ein ganzes Unternehmen stilllegen, indem dieser nur mit einem freundlichen Lächeln und einer gut erzählten Lüge Zutritt zu sensiblen Bereichen erhält.

## Schutzmaßnahmen

„Mir passiert das nicht!“

Natürlich, in diesem Moment, *genau jetzt*, da Sie wissen, welche Methoden ein Social Engineer sich zunutze macht, wird es schwierig sein, Sie dazu zu bringen, Ihr Passwort herauszugeben. Jetzt sind Sie informiert, wachsam – misstrauisch. Wie sieht es aber morgen aus? Wenn Sie durch den ganzen Alltagsstress nicht mehr wissen, wo oben und wo unten ist? Wenn eine Bitte hereinflattert und Sie diese einfach abwinken, weil Sie gerade Wichtigeres zu tun haben? Das sind die Momente, in denen unsere Achtsamkeit bröckelt. Das sind die Momente, auf die ein Social Engineer wartet.

Klar, wir haben alle eine hohe Selbstachtung vor uns selbst und der Gedanke, manipuliert zu werden, lässt uns mit einem unguuten Gefühl zurück, darum reden wir uns gern ein, dass wir nicht zu manipulieren sind. Dennoch sollte man sich eingestehen, dass es menschlich ist, anfällig zu sein – jeder Einzelne von uns. Gerade hier sind Awareness-Schulungen, bei denen Trainingsfragen gestellt werden, wichtig, um Misstrauen zu triggern. Solche Fragen sind:

- Kenne ich diese Person, die diese Anfrage stellt, und habe ich einen validen Grund, ihr zu vertrauen?
- Ist diese Person tatsächlich ein autorisierter Vertreter der Organisation, für die sie sich ausgibt?
- Warum erfolgt die Kontaktaufnahme nicht über den üblichen oder sicheren Kanal?
- Wieso wird Druck ausgeübt?
- Wieso will die Person sensible Informationen von mir haben?
- Wieso habe ich ein komisches Bauchgefühl bei dieser Person?

Der Angreifer wird bemüht sein, alle Warnsignale zu minimieren, und vermutlich schafft er es auch zu einem gewissen Grad. Wir erinnern uns: Social Engineers gehen subtil vor, unvorbereitet werden sie wohl selten vor Ihnen stehen. Sie wappnen sich für schwierige Situationen, und dennoch ist es nicht vollkommen hoffnungslos. Awareness ist hier wohl ein gutes Stichwort. Regelmäßige Schulungen helfen, eine Risikominderung zu erreichen. Gerade Unternehmen mit vielen Mitarbeitern – was zahlreiche potenzielle Schwachstellen impliziert – sollten konstante Schulungen in Betracht ziehen. Zum Schutze des Unternehmens, aber natürlich auch zum Einhalten von Compliance-Anforderungen.

<sup>1</sup> [https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html)

Lebensmittelunternehmer sollten ein besonderes Interesse an der Informationssicherheit haben, und das aufgrund mehrerer Gründe:

- **Schutz sensibler Kundendaten und Unternehmensgeheimnisse:** Lebensmittelunternehmen sammeln oft persönliche Daten von Kunden, einschließlich Zahlungsinformationen und Bestellhistorie. Um einen wirtschaftlichen Schaden zu vermeiden, braucht es den Schutz von Rezepturen, Lieferketteninformationen und anderen geschäftskritischen Daten. Das führt ebenfalls dazu, dass das Vertrauen der Kunden bewahrt und allen rechtlichen Verpflichtungen nachgekommen wird.
- **Vermeidung von Geschäftsausfällen:** Social Engineering Angriffe und Cyberangriffe können Produktions- und Lieferketten unterbrechen. Ein besonderer Fokus auf Informationssicherheit hilft, Betriebsstörungen zu verhindern.
- **Notfallpläne:** Effektive Informationssicherheit umfasst auch die Vorbereitung auf den Ernstfall, um den Geschäftsbetrieb schnell wieder aufnehmen zu können.
- **Einhaltung gesetzlicher Vorgaben:** Es müssen verschiedene gesetzliche Vorgaben und Standards in Bezug auf Datensicherheit und Verbraucherschutz eingehalten werden, bspw. wird das in der NIS-2-Richtlinie definiert. Dazu später mehr.
- **Sicherheit der Produkte:** Um die Integrität und die Sicherheit von Lebensmitteln zu gewährleisten, spielt die Informationssicherheit eine bedeutende Rolle. Verunreinigungen der Produkte durch Angriffe auf das Unternehmen können schwerwiegende Folgen haben.
- **Reputationsschutz:** Sicherheitsvorfälle können das Vertrauen der Verbraucher in ein Unternehmen stark beeinträchtigen. Ist die öffentliche Wahrnehmung einmal erschüttert, ist es schwer, diese wieder positiv aufzubauen.
- **Kostenreduktion:** Präventive Maßnahmen zur Informationssicherheit können langfristig Kosten senken, indem teure Datenpannen und Betriebsunterbrechungen verhindert werden.

Unter anderem fällt der Sektor „Ernährung“ in einige Richtlinien und Regularien:

## Gesetzliche Anforderungen an Unternehmen

### NIS-2-Richtlinie<sup>2</sup>

Die NIS-2-Richtlinie, welche offiziell ab Oktober 2024 in Kraft tritt und umzusetzen ist, betrachtet den Lebensmittelsektor als Teil der kritischen Infrastruktur (KRITIS), da Störungen in diesem Bereich erhebliche Folgen für die öffentliche Gesundheit und Sicherheit haben können. Unternehmen, die in diesem Sektor tätig sind, erbringen wesentliche Dienstleistungen, deren Ausfall zu bedeutenden wirtschaftlichen und gesellschaftlichen Schäden führen könnte.

Die Richtlinie definiert besondere Anforderungen, die Unternehmen im KRITIS-Bereich zu erbringen haben:

- **Sicherheitsanforderungen:**
  - Durchführung von Risikobewertungen
  - Umsetzung geeigneter Sicherheitsmaßnahmen
  - Management und Meldung von Sicherheitsvorfällen
- **Meldepflicht:** Es besteht eine verbindliche Pflicht zur Meldung von Cybervorfällen und Sicherheitsverletzungen an die zuständigen nationalen Behörden. Dies ermöglicht eine schnelle Reaktion und Koordination bei Sicherheitsvorfällen und reduziert das Risiko von Störungen in der Lebensmittelversorgungskette.
- **Kooperation und Informationsaustausch:** Die Richtlinie fördert die Zusammenarbeit und den Informationsaustausch zwischen Akteuren im Lebensmittelsektor sowie mit nationalen und europäischen Behörden. Dies beinhaltet den Austausch von Informationen über Bedrohungen, Schwachstellen und bewährte Verfahren, um die kollektive Sicherheit zu stärken.
- **Sanktionen und Durchsetzung:** Verstöße gegen die NIS-2-Richtlinie können erhebliche Sanktionen nach sich ziehen, einschließlich finanzieller Strafen. Unternehmen im Lebensmittelsektor müssen daher sicherstellen, dass sie alle Anforderungen der Richtlinie erfüllen.

<sup>2</sup> <https://www.openkritis.de/eu/eu-nis-2-sektoren-rce-cer.html#nis2-annex2>

Das Ziel dieser Richtlinie ist es, die Widerstandsfähigkeit und Sicherheit des Lebensmittelsektors gegen Bedrohungen und Informationssicherheitsrisiken zu verbessern, sodass Unternehmen in diesem Bereich gut auf Sicherheitsvorfälle vorbereitet sind.

**Der Aspekt der physischen Sicherheit:** Die NIS-2-Richtlinie der EU befasst sich primär mit der Cyber- und Informationssicherheit, jedoch erkennt sie auch die Bedeutung der physischen Sicherheit im Zusammenhang mit dem Schutz kritischer Infrastrukturen an. Um einen ganzheitlichen Schutz zu gewährleisten, müssen sowohl digitale als auch physische Sicherheitsmaßnahmen integriert werden. Dies bedeutet, dass Unternehmen nicht nur ihre IT-Systeme, sondern auch ihre physischen Räumlichkeiten und Anlagen zu schützen haben. Das Risikomanagement umfasst dementsprechend auch die physischen Bedrohungen.

### **KRITIS-Dachgesetz<sup>3</sup>**

Das KRITIS-Dachgesetz zielt darauf ab, die Sicherheit kritischer Infrastruktur zu erhöhen. Es legt fest, welche Sektoren als kritisch gelten, darunter Energie, Wasser, Ernährung<sup>4</sup>, Gesundheit und IT, und definiert Maßnahmen zur Verbesserung der Informationssicherheit.

Auch hier finden sich ähnliche Anforderungen zur NIS-2-Richtlinie unter anderem:

- **Physische Sicherheitsmaßnahmen:** Geeignete physische Sicherheitsvorkehrungen müssen getroffen werden, um unbefugten Zugang und physische Angriffe zu verhindern. Dazu gehören Maßnahmen wie Zugangskontrollen, Überwachungssysteme, Alarmanlagen und physische Barrieren.  
Kritische Standorte, z. B. Standorte, die für die Aufrechterhaltung wesentlicher Dienstleistungen wichtig sind, erfordern besondere Aufmerksamkeit. Diese müssen durch robuste physische Sicherheitsmaßnahmen geschützt werden.
- **Vorfalldmanagement:** Notfallhandpläne und Maßnahmen zur Reaktion auf physische Sicherheitsvorfälle sind zu entwickeln und zu implementieren. So kann sichergestellt werden, dass physische Angriffe oder Zwischenfälle schnell und effektiv gehandhabt werden.
- **Berichtspflichten:** Die NIS-2-Richtlinie schreibt vor, dass Sicherheitsvorfälle gemeldet werden müssen, das unterliegt ebenfalls dem KRITIS-Dachgesetz. Bei Vorfällen muss eine Meldepflicht an die zuständigen Behörden erfolgen. Die Kooperation mit Behörden wird somit zur Pflicht.

Das KRITIS-Dachgesetz stellt sicher, dass physische Aspekte umfassend berücksichtigt werden, um die Resilienz und den Schutz kritischer Infrastruktur in Deutschland zu gewährleisten. Das Gesetz tritt voraussichtlich im Frühjahr 2025 in Kraft. Die Betreiber kritischer Infrastruktur haben bis 17. Juli 2026 Zeit, die Vorgaben zu erfüllen. Darunter fällt der Sektor Ernährung<sup>5</sup>.

3 <https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html>

4 [https://www.openkritis.de/it-sicherheitsgesetz/sektoer\\_ernaehrung.html](https://www.openkritis.de/it-sicherheitsgesetz/sektoer_ernaehrung.html)

5 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227>



**DLG e.V.**

**Fachzentrum Lebensmittel**

Eschborner Landstraße 122 · 60489 Frankfurt am Main

Tel. +49 69 24788-311 · Fax +49 69 24788-8311

FachzentrumLM@DLG.org · www.DLG.org