Sicherheitsregeln, die im Betrieb wirklich wirken

Ein praxisnahes Schutzkonzept für den Mittelstand

Derek Carson · carson.de · derek@carson.de · November 2026

Was, wenn Ihre Beschäftigten den Angriff nicht erkennen?

Eine überzeugende Phishing-Mail. Ein Anruf mit der Stimme des Geschäftsführers. Eine dringende Bitte, die Bankverbindung eines Lieferanten zu ändern.

Solche Angriffe schlagen regelmäßig durch. Nach dem Bitkom-Bericht Wirtschaftsschutz 2026 beziffern deutsche Unternehmen ihren Schaden durch Diebstahl, Spionage und Sabotage auf 211 bis 271 Milliarden Euro; 76 Prozent davon entfallen auf Cyberangriffe. Ein Viertel der 1.003 befragten Unternehmen hatte in den letzten zwölf Monaten einen Schaden durch Ransomware, 16 Prozent einen Schaden durch Phishing.

Selbst gut geschulte Beschäftigte können auf solche Angriffe hereinfallen. Das ist kein individuelles Versagen, sondern eine Grenze jeder Schulung, die allein auf das Erkennen von Gefahren setzt.

Entscheidend ist deshalb eine andere Frage: Was passiert, wenn jemand getäuscht wird? Gibt es Regeln und Abläufe, die verhindern, dass aus einem Fehler ein Schaden entsteht? Können Beschäftigte einen Verdacht einfach melden? Und lässt sich überprüfen, ob diese Regeln im Alltag tatsächlich eingehalten werden?

Dieses Papier zeigt am Beispiel eines produzierenden Unternehmens, wie sich ausgewählte Informationssicherheitsrisiken in konkrete betriebliche Regeln, geeignete Maßnahmen und passende Schulungen übersetzen lassen – und wie sich ihre Umsetzung überprüfen lässt.

Warum der Zettel mit den Unterschriften nicht reicht

Das BSI-Gesetz verpflichtet die Geschäftsführungen wichtiger und besonders wichtiger Einrichtungen, regelmäßig an Schulungen teilzunehmen (§ 38 Abs. 3 BSIG). Die ISO/IEC 27001 verlangt darüber hinaus eine organisierte Sicherheitsarbeit, in der alle Mitarbeitenden die Regeln kennen, ihren eigenen Beitrag kennen und wissen, was bei Verstößen auf dem Spiel steht.

Der einfachste Nachweis für beides ist eine Teilnehmerliste. Sie belegt, wer im Raum war, und sonst nichts; ob danach auch nur eine Person anders handelt, steht nicht darauf. Der Schaden entsteht aber durch Handlungen. Eine Phishing-Mail richtet erst dann etwas an, wenn jemand auf den Link klickt oder Zugangsdaten eintippt; ein Zahlungsbetrug gelingt erst, wenn jemand eine Bankverbindung ungeprüft ändert oder eine Überweisung freigibt.

Was Studien über übliche Schulungen zeigen

Bei UC San Diego Health, einem großen Klinikverbund in den USA mit rund 19.500 Beschäftigten, wurde acht Monate lang untersucht, ob übliche Schulungen dieses Handeln ändern (Ho u. a., IEEE Symposium on Security and Privacy 2025). Die Teilnahme an der jährlichen Pflichtschulung zur Informationssicherheit führte nicht zu einem sichereren Umgang mit simulierten Phishing-E-Mails. Darüber hinaus senkte das Anzeigen einer kurzen Schulung direkt nach einem Fehlklick die zukünftige Klickrate nur um durchschnittlich 1,7 Prozentpunkte; mehr als die Hälfte dieser Schulungen wurde innerhalb von zehn Sekunden wieder geschlossen.

Eine zweite Studie lief 15 Monate lang in einem unbenannten großen Unternehmen mit mehr als 14.000 Beschäftigten (Lain, Kostiainen und Čapkun, ETH Zürich, IEEE Symposium on Security and Privacy 2022). Auch diese Studie zeigte: Schulungshinweise nach einem Fehlklick machten die Beschäftigten nicht widerstandsfähiger, teils sogar anfälliger.

Beide Studien zeigen, warum bestimmte Schulungsmaßnahmen wenig bewirken: Sie setzen voraus, dass Beschäftigte eine Bedrohung erkennen und im entscheidenden Moment richtig reagieren. Die jährliche Pflichtschulung soll das nötige Wissen dafür im Voraus vermitteln. Der Hinweis nach einem Fehlklick soll das Verhalten unmittelbar danach korrigieren. Beides gelingt jedoch nicht zuverlässig.

Erfolgreicher war in der zweiten Studie eine andere Maßnahme: Das Hinzufügen einer Meldetaste im Mail-Client führte zu einer stark erhöhten Wahrscheinlichkeit, dass simulierte Phishing-Mails an die IT-Sicherheit gemeldet wurden. Dafür mussten die Beschäftigten nicht selbst beurteilen, ob eine Nachricht tatsächlich ein Phishing-Versuch war. Sie konnten eine verdächtige E-Mail einfach melden; die IT-Sicherheit prüfte den Fall und konnte neue Angriffe frühzeitig erkennen. Die Meldung wurde damit zu einer einfachen Handlung, die keine sichere Einschätzung der Bedrohung voraussetzte.

Für die Gestaltung eines Sicherheitsprogramms ergibt sich daraus eine wichtige Konsequenz: Es reicht nicht, Wissen zu vermitteln und darauf zu hoffen, dass Beschäftigte es im Ernstfall richtig anwenden. Wirksamer sind klar definierte Regeln und Abläufe, die auch dann funktionieren, wenn jemand eine Bedrohung nicht erkennt oder unsicher ist. Daraus folgen drei Grundsätze:

- Abläufe, bei denen sicheres Handeln der normale und einfachste Weg ist.
- Mechanismen, die im Zweifelsfall ein einfaches, konstruktives Handeln ermöglichen und so Urteilsfehler reduzieren.
- Messungen, die zeigen, was im Betrieb tatsächlich geschieht, statt nur die Teilnahme an Schulungen zu dokumentieren.

Die zitierten Studien untersuchen Phishing. Die daraus gewonnenen Erkenntnisse lassen sich jedoch als Gestaltungsprinzip auf weitere Bereiche übertragen, in denen Beschäftigte unter Unsicherheit oder Zeitdruck Entscheidungen treffen müssen – etwa bei Zahlungsbetrug, Social Engineering per Anruf oder beim Umgang mit KI-Tools. Auch dort können klare Regeln und festgelegte Abläufe verhindern, dass die Sicherheit allein von der richtigen Einschätzung einzelner Beschäftigter abhängt. Die konkreten Maßnahmen in diesen Bereichen stützen sich auf etablierte Ansätze der Betrugsprävention, des internen Kontrollsystems und der betrieblichen Praxis, nicht auf die genannten Phishing-Studien.

Was dieses Konzept leistet — und was nicht

Die Forschung zur Informationssicherheit in Unternehmen ist umfangreich und zeigt reproduzierbare Befunde: Bestimmte Interventionen wirken messbar, andere nicht. Geschäftsführungen und Informationssicherheitsbeauftragte können sich auf diese Befundlage stützen, um erreichbare Programmziele von unerreichbaren zu trennen. Dieses Papier zieht diese Grenze explizit und beschreibt ein Sicherheitsprogramm, das sich auf Hebel konzentriert, die auf dokumentierter Evidenz und bewährter Praxis aufbauen.

Es unterscheidet dabei verschiedene Hebel, die im Alltag oft vermischt werden: **Awareness** (Wissen um die Bedrohung), **Schulung** (Üben einer konkreten Handlung), **organisatorische Regeln**, **operative Abläufe**, **technische Mechanismen** und **Management-Entscheidungen**. Das Konzept nutzt sie in Kombination; die Studien belegen vor allem die Grenzen der ersten beiden und die Wirkung bestimmter Mechanismen.

Was es nicht leistet:

- Die Klickrate auf verdächtige E-Mails senken. Keine Schulung schafft das zuverlässig; technische Filterung senkt sie jedoch nie auf null.
- Die individuelle Erkennungsfähigkeit der Beschäftigten verbessern. Ein gut gemachter Angriff täuscht auch geschulte Augen.
- Technische Maßnahmen ersetzen (Mail-Gateway, phishing-resistente MFA, EDR, isolierte Browser-Umgebungen). Die bleiben Aufgabe der IT.
- Schutz vor allen Angriffen bieten. Für den „resistenten Kern” von Wiederholungsklickern braucht es operative Zugriffskontrollen, keine zusätzliche Schulung.

Was es leistet:

- Abläufe verankern, in denen sicheres Handeln der normale Weg ist — etwa Rückruf vor Bankverbindungsänderung, Zwei-Personen-Freigabe bei Zahlungen oder keine Zahlungsfreigabe allein per Anruf. Messbar per Stichprobe im Betrieb.
- Einen funktionierenden Meldeweg für verdächtige E-Mails etablieren, damit das Unternehmen neue Angriffskampagnen früh erkennt. Messbar per Melderate.
- Den Schaden pro erfolgreichem Klick klein halten: Werden die Rückruf-Regel und die Regel „keine Zahlungsfreigabe allein per Anruf" eingehalten, führt ein BEC-Angriff per Mail nicht zu einer Falschüberweisung, und ein Deepfake-Anruf läuft ins Leere.
- Dokumentation liefern, die bei der Darstellung von NIS-2-Compliance und bei der Argumentation zur Haftungsentlastung der Geschäftsführung (§ 38 Abs. 2 BSIG) verwendet werden kann.

Das Arbeitsbeispiel

Die Muster Antriebstechnik GmbH im Arbeitsbeispiel ist ein erfundener Maschinenbauer in Osthessen mit 250 Beschäftigten. Dass das Unternehmen unter NIS-2 fällt, ist eine Annahme des Beispiels und keine rechtliche Einordnung; bei einem echten Unternehmen muss diese Frage geprüft werden. Der Vorteil eines erfundenen Unternehmens: Alle Unterlagen lassen sich in voller Tiefe zeigen, ohne vertrauliche Daten eines Kunden offenzulegen. Das Beispiel umfasst ein Sicherheitsprogramm mit Regeln und Abläufen sowie ein Schulungskonzept für vier Zielgruppen; alle Unterlagen sind enthalten, von den Leitfäden für die Trainer bis zu den Bewertungsbögen.

Vom Risiko zur Regel

Jede Regel im Programm geht von einem Risiko aus, das das Unternehmen bewertet hat, nicht von einem Themenkatalog. Stuft die Risikobewertung etwa Zahlungsbetrug über gefälschte E-Mails von Lieferanten als hoch ein, folgt daraus eine Regel für die Buchhaltung: Eine Bankverbindung wird erst geändert, wenn die Änderung über die bereits hinterlegte Kontaktangabe bestätigt, dokumentiert und von einer zweiten Person freigegeben ist. Diese Regel übt die Schulung im Rollenspiel, und im Betrieb prüft jedes Quartal eine Stichprobe, ob sie eingehalten wird.

Vier Zielgruppen, vier Formate

Wer an der Maschine steht, hat keinen PC, aber vor Schichtbeginn kurz Zeit. Die Geschäftsführung muss strategisch entscheiden und braucht deshalb Übung im Entscheiden, kein E-Learning. Weil die Arbeitsplätze so verschieden sind, teilt das Konzept das Programm in vier Module, die auf diese Gruppen zugeschnitten sind. Jedes Modul bündelt für seine Gruppe die passende Mischung aus Regel-Einführung, Prozedur-Übung und organisatorischer Unterstützung:

- **Geschäftsführung (M1):** 90 Minuten Briefing im ersten Quartal, eine Entscheidungsübung (60 Minuten) im vierten Quartal. Geübt wird, Risiken abzuwägen, im Ernstfall selbst zu entscheiden oder mit klarem Auftrag zu übertragen und eine Zahlung nie allein auf einen Telefonanruf hin freizugeben.
- **Büroarbeitsplätze (M2a):** Eine 60-minütige Schulung und vier kurze Einheiten, über das Jahr verteilt. Im Mittelpunkt: verdächtige Mails melden und Daten nur in offiziell freigegebene KI-Tools eingeben.
- **Produktion und Logistik (M2b):** 15-Minuten-Kurzunterweisungen zu Schichtbeginn durch die Schichtleitung, ergänzt um Aushänge und ein Merkblatt in einfacher Sprache. Inhalt: keine fremden USB-Sticks an Maschinen und auf Ungewöhnliches achten.
- **Finanzen, Personal & Einkauf (M3):** Ein 150-minütiger Workshop mit Rollenspielen in Gruppen bis fünf Personen. Bank- und Gehaltsdaten werden nur noch geändert, wenn die Änderung über die bereits hinterlegte Kontaktangabe bestätigt und von einer zweiten Person freigegeben ist.

Regeln statt Erkennen

Mit KI lässt sich eine Stimme am Telefon fälschen, und die angezeigte Telefonnummer lässt sich ebenfalls fälschen. Wer eine Fälschung erkennen soll, hat deshalb schlechte Karten. Das Arbeitsbeispiel setzt stattdessen auf eine Regel, die auch dann schützt, wenn niemand die Fälschung erkennt: Eine Zahlungsanweisung der Geschäftsführung gilt nie allein per Anruf, Sprachnachricht, Messenger oder Videokonferenz. Die Beschäftigten bestätigen sie über die Nummer im Telefonverzeichnis, die sie selbst wählen. Dieser Rückruf erreicht den echten Anschluss, auch wenn der erste Anruf dieselbe Nummer angezeigt hat.

Die Regel wirkt nur, wenn die Beschäftigten sich trauen, bei der Geschäftsführung nachzufragen. Deshalb gibt die Geschäftsführung sie selbst bekannt, in einem Rundschreiben mit dem Satz: „Wir halten uns selbst an diese Regel. Wenn wir eine Zahlung anweisen, rechnen wir mit Ihrem Rückruf.” Die Regel hält außerdem ausdrücklich fest, dass niemand einen Nachteil hat, der nachfragt, auch nicht bei einer echten Anweisung.

Melden ohne Nachteil

Die zweite Studie hat deutlich gemacht, wie wertvoll die Hinweise der Beschäftigten für das Unternehmen sind. Doch Beschäftigte melden nur dann offen, was ihnen auffällt, wenn sie keine Nachteile befürchten müssen. Deshalb steht in allen Modulen des Arbeitsbeispiels derselbe Satz: „Wer etwas meldet, auch einen eigenen Fehler, hat keinen Nachteil.” Dieser Satz wird allerdings erst verwendet, wenn die Geschäftsführung ihn ausdrücklich bestätigt hat. Denn ein Versprechen, das im Arbeitsalltag nicht eingehalten wird, richtet mehr Schaden an, als gar keines zu geben.

Entscheidungen mit Folgen

Im ersten Quartal entscheidet die Geschäftsführung, wie sie mit den Risiken aus dem Bericht der Informationssicherheitsbeauftragten umgeht: Sie kann Maßnahmen beauftragen, Risiken übertragen, sie bewusst akzeptieren oder die Entscheidung mit einem festen Termin vertagen.

Im vierten Quartal spielt sie gemeinsam mit der IT-Leitung, der Produktionsleitung und der Informationssicherheitsbeauftragten einen Cyberangriff durch, bei dem Schadsoftware die Produktion zum Stillstand bringt. Das Szenario knüpft an den tatsächlichen Stand im Unternehmen an – und damit auch an die Folgen der zuvor getroffenen Entscheidungen. Wurde eine beschlossene Maßnahme umgesetzt, versucht der Angreifer einen anderen Weg. Wurde sie nicht umgesetzt, bleibt die Sicherheitslücke bestehen.

Nach 32 Minuten meldet sich ein Anrufer mit der Stimme eines Geschäftsführers und fordert eine dringende Zahlung. In diesem Moment zeigt sich, ob die im ersten Quartal beschlossenen Regeln und Maßnahmen auch Monate später noch greifen.

Messen, was zählt

Jedes Modul wird auf zwei Arten überprüft:

1. **Lernzielkontrolle:** Der Trainer prüft nach einer vorher festgelegten Regel, ob die Vorgaben angewendet werden; im Buchhaltungs-Workshop lautet sie zum Beispiel: Wird die Kontoverbindung wirklich erst nach Rückruf über die hinterlegte Nummer geändert? Wo es darauf ankommt, ist festgelegt, welche Fehler so schwer wiegen, dass das Lernziel nicht bestanden ist. Wer ein Lernziel nicht besteht, wiederholt es mit neuen Fällen, zuerst allein, danach mit einem Gespräch.
2. **Betriebskennzahl:** Das Unternehmen zieht jedes Quartal eine zufällige Stichprobe und misst daran, ob die Abläufe im Alltag eingehalten werden, etwa ob bei jeder geänderten Bankverbindung Bestätigung, Freigabe und Änderung in dieser Reihenfolge dokumentiert sind.

Diese beiden Messungen belegen, ob gelernt wurde und ob die Regel im Betrieb umgesetzt wird. Zusammen gelesen zeigen sie außerdem, wo die Ursache liegt, wenn etwas nicht klappt: Haben alle das Lernziel bestanden und bleibt die Kennzahl trotzdem schlecht, liegt das Problem wahrscheinlich nicht am Wissen der Mitarbeitenden, sondern an einem technischen oder organisatorischen Prozess, etwa an einem System, das eine Änderung ohne Freigabe zulässt.

Datenschutz und Betriebsrat

Sobald Leistung oder Verhalten von Beschäftigten gemessen werden, berührt das den Datenschutz und die Mitbestimmung. Das Konzept baut deshalb von Anfang an Leitplanken ein. Gespeichert wird pro Person nur „bestanden" oder „nicht bestanden", ausgewertet wird erst ab Gruppen von zehn Personen. Vorgesetzte bewerten ihre Teams nicht selbst; die einzige Ausnahme sind die Schichtleitungen in der Produktion, die nach festen Regeln bewerten. Ein Klick in einer Phishing-Übung hat für die einzelne Person keine arbeitsrechtlichen Folgen und fließt in keine Beurteilung ein. Diese Leitplanken sind Vorschläge. Sie ersetzen weder die Prüfung durch die oder den Datenschutzbeauftragten noch die Abstimmung mit dem Betriebsrat, und eine Mindestgröße von zehn Personen schließt nicht in jedem Fall aus, dass sich Ergebnisse einzelnen Personen zuordnen lassen.

Freigabe vor dem Einsatz

Eine Regel, die in mehreren Unterlagen vorkommt, steht überall im selben Wortlaut, damit Trainer, Merkblatt und Bewertungsbogen dasselbe verlangen. Was das Unternehmen erst festlegen muss, etwa eine Frist, eine Telefonnummer oder den Weg für eine Meldung, ist als Muster gekennzeichnet und wird erst geschult, bewertet oder verteilt, wenn die Zuständigen es freigegeben haben. So lernt niemand eine Regel, die im Betrieb nicht gilt.

Welche Fragen das Beispiel beantwortet

- Was müssen wir bei der Schulung nachweisen, und was zeigt ein Nachweis wirklich?
- Welche Gruppe im Unternehmen braucht welche Regeln und welche Schulung, in welcher Form und wie lange?
- Wie schützen wir uns vor Betrug, den niemand erkennen kann?
- Woran erkennen wir, ob eine Regel im Betrieb eingehalten wird, und wo liegt die Ursache, wenn nicht?
- Wie messen wir, ohne Datenschutz und Betriebsrat zu übergehen?

Die Antworten gelten für dieses eine Unternehmen; für ein anderes werden Risiken, Gruppen und Regeln angepasst. Rechtsberatung enthält das Beispiel nicht. Ein fünftes Modul für den IT-Betrieb ist im Konzept geplant, aber nicht ausgearbeitet.

Das vollständige Arbeitsbeispiel

Das vollständige Arbeitsbeispiel umfasst auf 165 Seiten das Schulungskonzept und alle Unterlagen der Module M1, M2a, M2b und M3. Ein Auszug von 23 Seiten zeigt das Konzept bis Kapitel 3 und je eine Unterlage aus jedem Modul. Beides ist auf Anfrage direkt bei mir erhältlich: Derek Carson, derek@carson.de.

Quellen

- Bitkom e. V.: Wirtschaftsschutz 2026, Studienbericht.
- Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., Voelker, G. M.: Understanding the Efficacy of Phishing Training in Practice. IEEE Symposium on Security and Privacy 2025.
- Lain, D., Kostiainen, K., Čapkun, S.: Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. IEEE Symposium on Security and Privacy 2022.
- BSI-Gesetz (BSIG), §§ 38 und 65, Wortlaut auf gesetze-im-internet.de, geprüft am 02.11.2026.