

## Awareness-Training: Informationen für Betriebsräte

Liebe Mitglieder des Betriebsrates,  
wir kommen heute mit der Bitte um Zustimmung zum Awareness-Training auf Sie zu.

### Das ist Awareness-Training

Um den rechtlichen Anforderungen [u.A. Datenschutzgesetze] gerecht zu werden, die IT-Sicherheit der Mitarbeiter:innen zu stärken und etwaige Obliegenheitspflichten gegenüber Versicherungen [z.B. erweiterte Betriebshaftpflicht, IT-Risc, Data-Risc] zu erfüllen, planen wir die Durchführung eines Awareness-Trainings. Dieses Training zielt darauf ab, das Bewusstsein und die Fähigkeiten Ihrer Mitarbeiter:innen im Umgang mit IT-Risiken zu verbessern. Der Ansatz dabei ist auf dem Erlernen der notwendigen Fähigkeiten ausgerichtet.

Das Awareness-Training wird durch den externen Datenschutzbeauftragten [Hr. Schlütter von der net.ter GmbH] durchgeführt.

### Ziele des Trainings

- Rechtliche Anforderungen: Erfüllung gesetzlicher Vorgaben zur IT-Sicherheit [Sicherheit der Verarbeitung, Weisungen zum Umgang mit E-Mails und Internet],
- Stärkung der IT-Sicherheit: Sensibilisierung der Mitarbeiter für Phishing und andere IT-Risiken und
- Versicherungspflichten: Unterstützung bei der Einhaltung der Obliegenheitspflichten.

### Teilnehmer:innen des Trainings

- Führungskräfte und Mitarbeiter:innen, die Zugriff auf einen E-Mail-Account haben.

## Inhalte des Trainings

- Information der Teilnehmer:innen vor Beginn des Trainings: Wir stellen allen Teilnehmer:innen zu Beginn des Trainings eine umfassende Information zum Ablauf bereit. Dies erhöht den Lernerfolg aus dem Training wesentlich.
- Phishing-Simulationen: Mitarbeiter:innen erhalten gefälschte E-Mails, um ihre Fähigkeit zur Erkennung solcher Bedrohungen zu testen und zu verbessern. Diese E-Mails sind so gestaltet, dass sie realistische Phishing-Versuche nachahmen, jedoch keine tatsächliche Gefahr darstellen. Ziel ist es, die Mitarbeiter:innen zu schulen, verdächtige E-Mails zu erkennen und angemessen darauf zu reagieren.
- Schulungsmaterialien: Neben den Simulationen werden den Mitarbeiter:innen umfangreiche Schulungsmaterialien zur Verfügung gestellt. Diese beinhalten Informationen und Checklisten zur Erkennung von Phishing-E-Mails und anderen IT-Risiken. Die Materialien sind darauf ausgelegt, das Wissen der Mitarbeiter:innen kontinuierlich zu erweitern.
- Feedback und Nachschulung: Die Ergebnisse der Phishing-Simulationen werden dokumentiert und ausgewertet. Mitarbeiter:innen, die mehrfach auf gefälschte Links klicken, erhalten gezielte Nachschulungen, um ihre Sensibilität gegenüber IT-Risiken zu erhöhen. Dieses Feedback ist ein wichtiger Bestandteil des Trainings, um die Stärkung der Mitarbeiter:innen zu erreichen.

## Zusammenarbeit

Wir möchten Sie aktiv einbeziehen. Dazu gehört:

- Transparenz: Regelmäßige Informationen über den Fortschritt und die Ergebnisse des Trainings. Der Betriebsrat wird über alle wichtigen Schritte und Entwicklungen informiert, um eine transparente und offene Kommunikation zu gewährleisten.
- Gesamtauswertung: Der Betriebsrat erhält jährlich die Gesamtauswertung der Trainingsergebnisse. Diese Auswertung umfasst detaillierte Berichte über die Teilnahme, die Häufigkeit von Klicks auf gefälschte Links und die Wirksamkeit der Nachschulungen (alle Daten anonymisiert). Ziel ist es, die Effektivität des Programms zu bewerten und gegebenenfalls Anpassungen vorzunehmen, um die IT-Sicherheit kontinuierlich zu verbessern.

## Vorteile des Awareness-Trainings

- Erhöhte IT-Sicherheit: Durch die Sensibilisierung der Mitarbeiter für IT-Risiken wird die allgemeine IT-Sicherheit im Unternehmen erhöht. Mitarbeiter sind besser in der Lage, Phishing-Versuche zu erkennen und angemessen darauf zu reagieren, was das Risiko von Sicherheitsvorfällen reduziert.
- Erfüllung rechtlicher Anforderungen: Das Training hilft dabei, gesetzliche Vorgaben zur IT-Sicherheit zu erfüllen und das Unternehmen vor rechtlichen Konsequenzen zu schützen.
- Verbesserte Versicherungsbedingungen: Durch die Einhaltung der Obliegenheitspflichten gegenüber unserer Versicherung können wir möglicherweise bessere Versicherungsbedingungen erzielen und das Risiko von Versicherungsschäden minimieren.
- Stärkung des Sicherheitsbewusstseins: Das Training trägt dazu bei, ein allgemeines Bewusstsein für IT-Sicherheit im Unternehmen zu schaffen. Mitarbeiter werden ermutigt, verdächtige Aktivitäten zu melden und proaktiv zur Sicherheit des Unternehmens beizutragen.

Wir freuen uns auf eine konstruktive Zusammenarbeit und stehen für Rückfragen jederzeit zur Verfügung. Gemeinsam können wir die IT-Sicherheit in Ihrer Organisation nachhaltig verbessern und die Mitarbeiter:innen bestmöglich auf die Herausforderungen im Umgang mit IT-Risiken vorbereiten.

Mit freundlichen Grüßen aus Düsseldorf



Johannes Schlütter  
Datenschutzbeauftragter