Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Awareness stärken – Risiken minimieren

Awareness stärken – Risiken minimieren

Investieren Sie langfristig in die Sicherheit Ihres gesamten Unternehmens, indem Sie kontinuierlich das Informationssicherheitsbewusstsein Ihrer Mitarbeitenden schärfen.
Der „Sicherheitsfaktor Mensch“ spielt eine wichtige Rolle bei der Abwehr von Cyberangriffen. Geschultes Personal und eine sensibilisierte Belegschaft sind genauso relevant wie technische Maßnahmen. Informationssicherheit betrifft alle Ebenen des Unternehmens, von der Geschäftsführung bis zu den Mitarbeitenden in jeder Abteilung.

„Sicherheitsfaktor Mensch“

Der Mensch wird wegen Social-Engineering-Angriffen häufig als eine der größten Schwachstellen in der Informationssicherheit bezeichnet. Ungeschultes Personal stellt eine Herausforderung dar, die Sie als Management jedoch selbst bewältigen können.

Durch effektives Training und das richtige Wissen können Ihre Mitarbeitenden zu einem starken Schutzschild vor Cyberangriffen werden. Integrieren Sie Ihr Team als wesentlichen Bestandteil Ihrer Sicherheitsstrategie und verankern Sie diese in der Gesamtstrategie Ihres Unternehmens.

Auch im BSI-Grundschutz 200-2 wird betont, dass Sicherheitsmaßnahmen nur wirksam sein können, wenn die betroffenen Mitarbeitenden darin geschult werden.

Kommunizieren Sie offen die Relevanz von Sicherheitsmaßnahmen auf verschiedenen Ebenen und die Verantwortung jedes Einzelnen über die IT-Abteilung hinaus!

Wenn Sie als Führungskraft die Initiative ergreifen und Sicherheit vorleben, indem Sie sich strikt an Ihre eigenen Sicherheitsmaßnahmen halten, erhöht dies auch die Motivation Ihrer Mitarbeitenden, zum Schutz des Unternehmens beizutragen, und sendet eine klare Botschaft.

Bei einem möglichen Vorfall sind es resiliente Mitarbeitende, die besonnen bleiben, ihr Fachwissen nutzen und engagiert daran arbeiten, das Unternehmen wieder auf Kurs zu bringen. Je schneller die Meldung und Reaktion auf einen Sicherheitsvorfall erfolgt, desto mehr Schaden kann verhindert werden.

Verankern Sie Awareness in Ihrer Unternehmenskultur durch …

… kontinuierliche Fortbildung

Das Entwickeln und Schulen eines Informationssicherheitsbewusstseins ist ein kontinuierlicher Prozess, der fest im Unternehmen verankert werden muss. Die Inhalte können variieren, sollten jedoch regelmäßig wiederholt werden. Informationen, die in kleinen „Paketen“ vermittelt werden, sind oft effektiver als umfangreiche Schulungen.

… Vermittlung in Form von Gamification, Infotainment und Simulationen

Geben Sie die Inhalte auf spielerische Art und Weise weiter und wählen Sie eine adäquate Ansprache für die jeweilige Zielgruppe. Dies motiviert und macht die Inhalte spannender. Stellen Sie einen Bezug zum (Arbeits-)Alltag her und geben Sie konkrete Tipps und Vorgaben für die gewünschte Vorgehensweise.

… transparente Kommunikation

Kommunizieren Sie die Regeln und deren Wichtigkeit kontinuierlich. Kommunizieren Sie außerdem Vorfälle und deren Bewältigung offen mit Ihren Mitarbeitenden, um deren Bewusstsein zu schärfen. Richten Sie einen Weg ein, über den Ihre Mitarbeitenden Sicherheitsvorfälle oder Verdachtsfälle unkompliziert melden können.

… eine positive Fehlerkultur

Eine positive Fehlerkultur ist entscheidend, damit sich Ihre Mitarbeitenden bei einem möglichen Vorfall vertrauensvoll an Sie wenden und diesen zeitig melden. Aus Fehlern lassen sich wertvolle Erfahrungen gewinnen.

Cyber-Awareness-Programm in 8 Schritten

Folgende acht Schritte, entwickelt von der European Union Agency for Cybersecurity – ENISA, helfen Ihnen, ein Cyber-Awareness-Programm zugeschnitten auf Ihr Unternehmen zu entwickeln:

1

Sensibilisierungsziele ermitteln

2

Finanzielle Mittel sicherstellen

3

Personelle Ressourcen sicherstellen

4

Zielgruppen identifizieren

5

Passende Methoden für Zielgruppe wählen

6


Zeitplan erstellen

7

Mit der Durchführung starten

8

Programm evaluieren und überarbeiten

NIS-2-Richtlinie

In der NIS-2-Richtlinie der EU wird die Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen aufgefordert, Informations- und Schulungsmaßnahmen anzubieten, um das allgemeine Bewusstsein der Mitarbeitenden für die Risiken im Zusammenhang mit IKT-Produkten zu schärfen. Außerdem soll das Management auch selbst regelmäßig an solchen Schulungen teilnehmen.

Die Etablierung von Cyber-Awareness-Maßnahmen ist also ein Schritt, der im Vorgriff auf die nationale Umsetzung der NIS-2-Richtlinie schon heute ergriffen werden kann.

BSI – Management Blitzlichter

NIS 2 – Unterstützungsangebote des BSI

ENISA – Awareness raising in a box

Impressum

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E Mail: bsi@bsi.bund.de
www.bsi.bund.de

Bildnachweis Adobe Stock/ Sawitree88

Stand Oktober 2024