

Mitarbeiter-Sensibilisierung in KMU

Technische und organisatorische Schutzmassnahmen sind wichtig, reichen aber für eine ganzheitliche Betrachtung der Informationssicherheit nicht aus. Mitarbeitende sollen die Technik korrekt bedienen und sich im Geschäftsalltag sicher verhalten. Deshalb spielen Schulungs- und Sensibilisierungsmassnahmen (sog. Awareness) für Mitarbeitende ebenfalls eine bedeutende Rolle und dürfen nicht vernachlässigt werden.

Wichtige Merkmale:

- Erstellen Sie einfach umzusetzende Benutzerrichtlinien.
- Sensibilisieren und schulen Sie Ihre Mitarbeitenden regelmässig und wiederkehrend.
- Nutzen Sie verschiedene Kommunikationskanäle und Hilfsmittel, um alle Mitarbeitenden zu erreichen.
- Bestärken Sie die Mitarbeitenden Auffälligkeiten, Verstösse etc. zu melden.

Warum ist Sensibilisierung in KMU wichtig?

Ein Blick in die Statistiken von erfolgreichen Cyberangriffen zeigt, dass der Faktor Mensch eines der häufigsten Einfallstore ist. Dabei wird mittels z.B. [Social Engineering](https://www.ebas.ch/social-engineering) (<https://www.ebas.ch/social-engineering>) oder [Phishing](https://www.ebas.ch/phishing) (<https://www.ebas.ch/phishing>) der Mensch dazu überlistet, sensitive Daten preiszugeben oder eine unerwünschte Aktion auszuführen. Erfahrungsberichte aus verschiedenen Unternehmen zeigen, dass es nicht genügt, Sicherheitsmassnahmen lediglich anzuordnen. Verstehen die Mitarbeitenden die Bedeutung und den Zweck der Sicherheitsmassnahmen nicht, werden diese nicht oder nur dürftig umgesetzt.

Um das Bewusstsein für Sicherheit unter den Mitarbeitenden zu schärfen und die Priorität von Informationssicherheit im Unternehmen hervorzuheben, sollten ganzheitliche, unternehmensweite Awareness-Aktivitäten stattfinden. Es gibt unterschiedliche Strategien, um eine Kultur der Sicherheit zu etablieren und zu formen. Für langanhaltenden Erfolg ist eine an die Zielgruppe angepasste, kontinuierliche wiederkehrende Kommunikation essenziell.

Wie gelingt die Sensibilisierung von Mitarbeitenden in KMU?

Es empfiehlt sich übersichtshalber, zur Minimierung der Kosten und zur Maximierung des Erfolges ein Awareness-Konzept zu erstellen. Dies muss nicht gross und umfangreich sein, sondern soll die Awareness-Aktivitäten aufeinander abstimmen und effizient gestalten. Sehr wichtig in diesem Zusammenhang ist, dass das Management hinter den Awareness-Aktivitäten steht und als Vorbild figuriert.

Mögliche Arten für mehr Awareness im Unternehmen sind:

- **Schulungen und Workshops:** Regelmässige Fortbildungen zu relevanten Themen helfen, die Mitarbeitenden auf dem neuesten Stand zu halten.
- **Interne Kommunikation:** Ein regelmässiger Austausch über Neuigkeiten, Änderungen oder wichtige Informationen fördert das Bewusstsein und das Verständnis der Mitarbeitenden.
- **Anlaufstelle und Feedback-Kultur:** Es ist wichtig, den Mitarbeitenden eine Anlaufstelle/Plattform zu bieten, auf welcher sie Auffälligkeiten und Verstösse melden, aber auch Bedenken äussern, sowie Fragen stellen oder

Vorschläge machen können.

- **Externes Expertenwissen:** Manchmal kann es hilfreich sein, externe Experten für spezielle Themen einzuladen, um tiefergehendes Wissen zu vermitteln.
- **Awareness-Plattform:** Auch können Sie sich als Unternehmen einer Awareness-Plattform anschliessen und so die Sensibilisierung im Unternehmen unterstützen.
- **Integration in die Unternehmenskultur:** Sensibilisierung darf nicht nur eine einmalige Aktion sein, sondern muss nachhaltig in die täglichen Arbeitsabläufe und die Unternehmenskultur integriert werden.

Abschliessend lässt sich sagen, dass die Sensibilisierung von Mitarbeitenden eine Investition in die Zukunft des Unternehmens ist. Sie schützt nicht nur vor rechtlichen Risiken und Reputationsverlust bei einem allfälligen Cybervorfall, sondern fördert auch ein positives Arbeitsumfeld und steigert die Produktivität. Im zunehmend stark digitalisierten Umfeld ist eine gute Sicherheitskultur im Unternehmen ein entscheidender Wettbewerbsvorteil.

Weitere Informationen

Das [Informationssicherheitshandbuch für die Praxis \(https://www.sihb.ch/\)](https://www.sihb.ch/) bietet gute Anleitungen und Mustervorlagen, unter anderem auch rund um das Thema Sensibilisierung von Mitarbeitenden. (Als Teilnehmer:in des [Kurses für KMU \(https://www.ebas.ch/kurs-fuer-kmu/\)](https://www.ebas.ch/kurs-fuer-kmu/) können Sie das Buch mit 30% Rabatt zum Vorzugspreis von CHF 68.– (exkl. Versandkosten) bestellen.)

«eBanking -aber sicher!» bietet für [KMU auch einen Online-Kurse \(https://www.ebas.ch/kurs-fuer-kmu/\)](https://www.ebas.ch/kurs-fuer-kmu/), um wichtige technische sowie organisatorische Massnahmen für KMU's zu beleuchten.

Unter «Awareness» wird im Kontext der Informationssicherheit verstanden, dass sich die Mitarbeitenden den Cybergefahren bewusst sind, und in der Lage sind sich sicher zu verhalten.

Da sowohl das externe (z.B. neue Angriffsvarianten), als auch das interne Umfeld (z.B. neue Prozesse oder Tools) einem ständigen Wandel unterworfen sind, muss Awareness zwingend als wiederkehrende Aufgabe verstanden und umgesetzt werden.