Training Integrale Sicherheit / Informationssicherheit

Produkte / Dienstleistungsumschreibung

Um an Informationen und Daten über hochentwickelte Technologien und Patente, über Kunden und Mitarbeitende, aber auch über eingespielte Prozesse oder Ähnliches zu gelangen, werden immer neue Varianten krimineller Aktivitäten entwickelt. Das Motiv ist entweder die finanzielle Beute oder die Schwächung des Unternehmens als Konkurrent. Mitarbeiterinnen und Mitarbeiter auf allen Hierarchieebenen mit ihren vielfältigen geschäftlichen und privaten sozialen Kontakten bieten eine breite Angriffsfläche, zumal sich die Unternehmen stark auf die Absicherung ihrer IT-Systeme gegen Cyber-Angriffe konzentrieren. Die ausgenutzte Schwachstelle, der Nutzer selbst, rückt zunehmend in den Fokus der Angreifer. Der Mensch mit seinem Verhalten ist somit das grösste Risiko für ein Unternehmen - einerseits in der Informationssicherheit, andererseits aber auch bei der Schaffung von Integraler Sicherheit.

NUTZEN	Markante Verbesserung des Risikobewusstseins und der Anwendung von abwehrenden Massnahmen in den Bereichen Informations- bzw. IT-Sicherheit, aber auch physische / personelle Sicherheit. Deutliche Reduktion der Verwundbarkeit gegenüber Angriffen und klare Erhöhung der Sicherheitsmaturität im gesamten Betrieb.
INHALT	▪ ½ Tag – Allgemeines Training (Fokus Informationssicherheit): ▪ Verschiedene Arten von Angreifern und Erkennen von Schwachpunkten ▪ Schwachstelle Mensch, Bedrohungen und Angriffsmethoden ▪ Gefälschte Infos/Nachrichten und versteckte Absichten erkennen/abwehren ▪ Open Source Intelligence (OSINT) und Social Engineering, schützendes Verhalten dazu ▪ Sicherheitsbewusster Umgang mit Informationen, geschäftlich & privat ▪ Individuelle Sicherheitsverantwortung erkennen und wahrnehmen ▪ 1 Tag – Zugeschnittenes Training (Integrale Sicherheit und Informationssicherheit im Unternehmen): ▪ Themen des allgemeinen Trainings - zusätzlich: ▪ Schärfung des Bewusstseins für das Kernwissen und die Assets des eigenen Unternehmens ▪ Der „rote Faden“ bei Angriffen / Cyberattacken (Kontaktaufnahme, Methodik und Angriffsmuster) ▪ Sicherheitsbewusstes Verhalten im direkten Personenkontakt und in der Kundenbetreuung ▪ Gesundes Misstrauen im Zusammenspiel mit freundlicher sozialer Interaktion ▪ Erkennen von Schwachstellen in Ihrem Unternehmen ▪ Physische Bedrohungen für Ihr Unternehmen und Ihre Mitarbeiter ▪ Konkrete Präventions- und Abwehrmassnahmen in Ihrem Unternehmen ▪ Praktische Übungen zur Risikominimierung
METHODIK	▪ Theoretische Inputs, Gruppenarbeit und Rollenspiele ▪ Individuelle Reflexion mit Austausch von Erfahrungen und bewährten Praktiken
ZIELGRUPPE	VR, GL, Kader, Mitarbeiter aller Stufen und aus allen Branchen. Gefährdet sind insbesondere: ▪ Entscheidungsträger und Personen mit besonderem Schlüsselwissen ▪ Personal in Kontakt mit Kunden, Partnern, Zulieferern, Lieferdiensten
DAUER / ORT	▪ 4 oder 8 Stunden inkl. Kurzpausen. Mittagspause bei Ganztageskurs zusätzlich. ▪ In Ihren Räumlichkeiten / Externe Kurslokationen nach Absprache.
KOSTEN	½ Tag: CHF 1‘900.00 für Gruppen bis 8 Teilnehmer CHF 3‘500.00 ab 9 bis max. 18 Teilnehmer (2 Kursleiter) 1 Tag: CHF 3‘300.00 für Gruppen bis 8 Teilnehmer CHF 5‘600.00 ab 9 bis max. 18 Teilnehmer (2 Kursleiter) (Preise: Trainingsgebühren, ohne Spesen, ohne Veranstaltungsort / Mittagsverpflegung)
LEITUNG	Chris Eckert, Thomas Winkler