Training Integrale Sicherheit / Informationssicherheit

Produkte / Dienstleistungsumschreibung

Zur Beschaffung von Informationen und Daten zu hochentwickelten Technologien und Patenten, zu Kunden und Mitarbeitenden, aber auch zu eingespielten Prozessen oder ähnlichem, werden immer neue Varianten von kriminellen Aktivitäten entwickelt. Das Motiv liegt entweder in der finanziellen Beute oder aber der Schwächung eines Unternehmens als Konkurrenz. Beschäftigte auf allen Hierarchieebenen mit ihren vielfältigen geschäftlichen und privaten sozialen Kontakten bieten eine breite Angriffsfläche, umso mehr, da Unternehmen sich stark auf die Absicherung ihrer IT-Systeme gegen Cyberattacken konzentrieren. Die ausgenutzte Schwachstelle, der Benutzer selbst, gerät 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 ▪ Aufzeigen und Wahrnehmen von individueller Sicherheitsverantwortung 1 Tag – Zugeschnittenes Training (Integrale Sicherheit und Informationssicherheit im Unternehmen): ▪ Themen des allgemeinen Trainings – zusätzlich dazu: ▪ Bewusstseinssteigerung zu Kernwissen und Sachwerten der eigenen Firma ▪ Der „rote Faden" bei Angriffen / Cyberattacken (Kontaktaufnahmen, Methodik und Angriffsmuster) ▪ Sicherheitsbewusstes Verhalten im direkten Personenkontakt und in der Kundepflege ▪ Gesundes Misstrauen im Zusammenspiel mit umgänglicher sozialer Interaktion ▪ Identifikation von Schwachstellen in Ihrem Unternehmen ▪ Physischen Bedrohungen für Ihren Betrieb und das Personal ▪ Konkrete Präventions- und Abwehrmassnahmen in Ihrer Firma ▪ 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 Gruppe bis 8 Teilnehmer CHF 5'600.00 ab 9 bis max. 18 Teilnehmer (2 Kursleiter) (Preise = Trainingsgebühren, ohne Spesen, ohne Veranstaltungsort / Mittagsverpflegung)
LEITUNG	Heinrich Schneider, Chris Eckert