ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

CyberUp: State of the Art Cybersecurity Awareness

1. Die Herausforderung

IT-Sicherheits(ITS)-Awareness-Maßnahmen stoßen in Unternehmen oft auf Widerstand und zeigen keine Erfolge durch

- **geringe Effektivität:** One-size-fits-all-Schulungen greifen zu kurz.
- **fehlende Relevanz:** Mitarbeitende erkennen nicht den direkten Nutzen für ihren Arbeitsalltag.
- **mangelnde Motivation:** Trainings sind oft abstrakt, langatmig oder wenig interaktiv.
- **unklare Kompetenzbedarfe:** Wer muss was genau wissen?

2. Die Kernbausteine eines modernen Awareness-Programms

Ein effektives Awareness-Training muss sich an den unterschiedlichen Kompetenzstufen der Mitarbeitenden orientieren:

- **Konzeptionelle Kompetenz:** Vermittlung von regelbasiertem, abstraktem Wissen über ITS-Maßnahmen.
- **Prozessuale Kompetenz:** Training von Verfahren und Fähigkeiten zur Anwendung von IT-Sicherheitsmaßnahmen.
- **Interpretierende Kompetenz:** Förderung der Fähigkeit, Bedrohungssituationen zu erkennen und richtig zu interpretieren.
- **Motivationale Kompetenz:** Entwicklung einer sicherheitsbewussten Haltung und Motivation zur proaktiven Anwendung von IT-Sicherheitsmaßnahmen.

3. Mögliche Umsetzung in Awareness-Programm

Messung & Kontinuierliche Verbesserung

- Mitarbeiterspezifische Sensibilisierung durch individuelle annonymisierte Risiko-Analysen.
- Benchmarking des Sicherheitsverhaltens gegen über Branchenstandards.

Adaptive & Personalisierte Schulungen

- Lernplattformen analysieren den Lernfortschritt.
- Rollenbasierte Schulungen für Geschäftsführung, IT-Admin, medizinisches Fachpersonal etc.

Micro-Learning & Just-in-Time Training

- Kurze, alltagstaugliche Lerneinheiten (z. B. 5-Minuten-Videos, Quizze).
- Sicherheits-Tipps in Arbeitsprozesse integriert, z.B. über Chatbots

Security Nudging & Verhaltenspsychologie

- Automatische Hinweise bei riskanten Aktionen (z. B. unsichere E-Mail-Anhänge).
- Kleine, gezielte Erinnerungen zur Förderung sicherer Verhaltensweisen.
- Live-Demos von Cyberangriffen zur Veranschaulichung aktueller Bedrohungen.

Jemand ist in einem Bereich **gut qualifiziert** durch:

Was?	**Konzeptionelle Kompetenz**	Regelbasiertes, abstraktes Wissen in einem Bereich.
↓		
Wie?	**Prozessuale Kompetenz**	Wissen über Verfahren und Fähigkeiten, die erfoderlich sind, um konzeptionelles Wissen in bestimten Handlungssituationen anzuwenden.
↓		
Wann?	**Interpretierende Kompetenz**	Kognitives Erkennen der Anforderungs-situation und Wissen über angemessene Interpretation und Valididerung der Situation.
↓		
Warum?	**Motivationale Kompetenz**	Grundlegende motivationale und affektive Merkmale in bestimmten Handlungs-situationen.

Kostenloser Test für KMUs zu profilspezifischen Cybersicherheitskompetenzen: https://itskompetent.uni-goettingen.de/getstarted

Handout zur Präsentation: Wirkungsvolle Umsetzung von IT-Compliance & -Awareness von Dr. Kristin Masuch, CEO und Gründerin der CySec GmbH und Dozentin für Informationssicherheit an der Universität Göttingen

EDITH GERMANY
Enabling Digital Innovation & Technology in Hesse

Co-funded by the European Union