SECURITY ARENA

DAS AWARENESS CIRCLE TRAINING OUT OF THE BOX

KATAQLOG 2020 JETZT MIT 30 STATIONEN

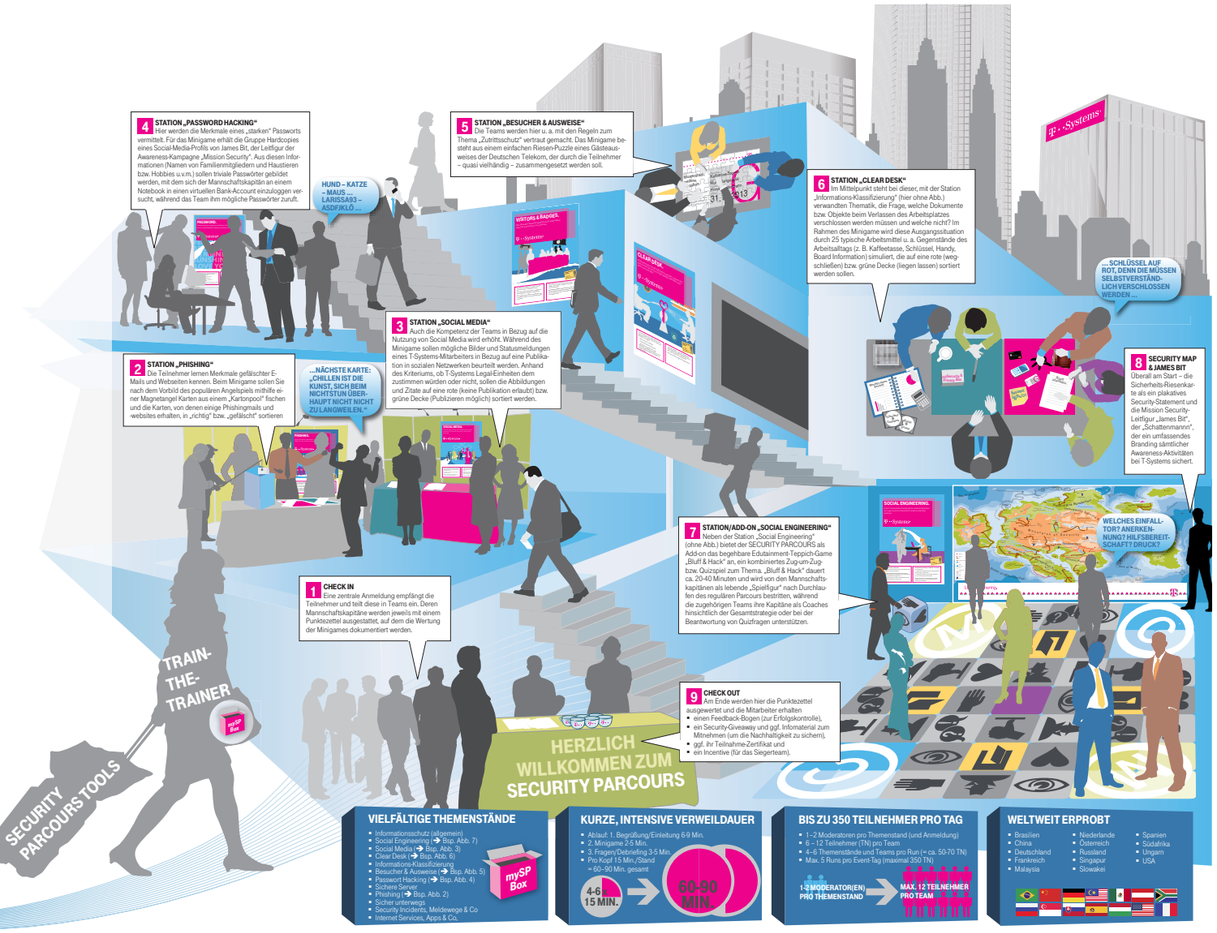
IT-Sicherheitspreis NRW 2007
für askit by known-sense

Sicherheitsforum Baden-Württemberg
Die Wirtschaft schützt ihr Wissen
Sicherheitspreis Baden -Württemberg 2011 für Cytec-Audio-Podcasts

Information Security Forum
Most innovative Awareness Campaign 2013: „SECURITY PARCOURS“ by T-Systems – supported by known_sense

Outstanding Security Performance Award (OSPA) 2015: „Herausragende Initiative für Sicherheitsschulungen“ für „SecurityArena“ by known_sense

known_sense
awareness you can touch.



INTERAKTIVES LERNEN IM TEAM UND DIE ROLLEN-BASIERTEN SPIELE INNERHALB EINES PARCOURS ERZEUGEN DIE NOTWENDIGE BEWEGUNG

Security Arena – Awareness Training als eine gute, verbindende Geschichte nach dem Prinzip „Talking Security“.

Wie gestalte ich Security-Trainings, die bleibende Awareness schaffen und gleichzeitig auch noch Spaß bereiten? Die Antwort heißt „Awareness Next Generation“ und greift in ihrem methodischen Ansatz bereits die aktuellen Herausforderungen von Information Security auf: Social Engineering. Das „soziale Element“ ist damit sowohl Gefahr wie zugleich auch der Schlüssel für Beteiligung und Nachhaltigkeit und wird von uns im Rahmen der sog. Security Arena berücksichtigt. Die Security Arena ist eine von T-Systems und known_sense gemeinsam entwickelte Roadshow mit einem Awareness-Circle-Training nach der Methode des Stationenlernens.

Bei der Security Arena durchlaufen Teams mit 3 bis 12 Teilnehmern synchron 4-6 Themenstationen, an denen sie von Moderatoren hinsichtlich verschiedener Sicherheits-Themen sensibilisiert werden. Jede der derzeit angebotenen Stationen dauert lediglich 15 Minuten und beinhaltet u. a. jeweils ein „Minigame“, das mit den anderen Games und Moderatoren-Briefings in einen handelsüblichen Koffer passt. Moderiert wird stets von Kollegen (d. h. „Laien“) auf Basis eines Train-the-Trainer-Konzepts. An jeder Station können die Teams Punkte sammeln und am Ende einen Teampreis gewinnen. Nach jeweils 15 Minuten und den stets identischen drei Phasen (Einleitung – Minigame – Debriefing) wird die Station gewechselt. So können während eines Sicherheits-Event täglich bis zu 350 Mitarbeiter mit Brennpunktrisiken und deren Abwehr vertraut gemacht werden.

4 Themen in nur 60 Minuten

Die Security Arena hat sich seit 2011 an in mehr als 25 Ländern auf allen 5 Kontinenten bewährt – von Brasilien bis Australien, von Südafrika bis nach Russland. 2013 wurde der Arena Line Extender „SECURITY PARCOURS“ vom ISF (International Security Forum) als weltweit „innovativste Awareness-Kampagne“ ausgezeichnet. 2015 erhielten known_sense und die Security Arena den OSPA (Outstanding Security Performance Award, Kategorie „Herausragende Initiative für Sicherheitsschulungen“).

Security Arenen werden bei unseren Lizenznehmer in der Regel lokal organisiert, wobei jede Einheit ihr Arena-Event unabhängig mit angepassten Inhalten, eigenen Moderatoren und eigenen Marketingmitteln durchführt. known_sense stellt mit dem zentralen Sicherheitsmanagement jedes Kunden Methoden, (didaktischen) Content und Event-Support als Unterstützung des lokalen Sicherheitsmanagements zur Verfügung. Das komplette Material für alle Stationen samt dazugehörigem Supportmaterial (z. B. Promotionoder Themenposter, diverse Event-Organisations-Templates) passt in einen handelsüblichen Koffer – eine Roadshow ‚out of the box‘! Jedes Jahr werden von uns mindestens zwei neue Themenstationen kreiert; inzwischen sind auch ein „Digital Parcours“ und Stationen zum Thema personelle Sicherheit kurz vor dem Launch.

Was unterscheidet die Security Arena von klassischen Trainings?

Im Gegensatz zur Online-Sensibilisierung mithilfe eines WBTs, das bei aller Selbstbestimmtheit relativ „einsam“ stattfindet, hebt z. B. die Security Arena Awareness von der kognitiven Ebene der Informationsvermittlung auf die für das Lernen so wichtige Beziehungsebene. Der Einzelne profitiert dabei von der emotionalen Aufladung innerhalb der Gruppe. Denn soziale Teilhabe

führt zu einem höherem Involvement, mehr Lebendigkeit und zu einer ganzheitlichen Awareness, bei der einzelne Lernschritte vor allem über die Interaktion mit Erlebnissen belegt werden und auf diesem Weg (diskursives Lernen) eine bessere Resilienz und Memorierbarkeit erzielt werden. D. h. die Security Arena bildet Gesprächsthemen und bringt Sicherheit nach dem Prinzip „Talking Security" in einen permanenten kommunikativen Umsatz.

Derzeit verfügbare Stationen:

- Datenschutz (2 verschiedene Spiele) S. 6
- Clear Desk S. 8
- Informations-Klassifizierung S. 10
- Passwort Hacking S. 12
- Besucher & Ausweise (2 verschiedene Spiele) S. 14
- Social Media S. 16
- Social Engineering S. 18
- Phishing S. 20
- Sicher unterwegs S. 22
- Sichere Server S. 24
- Incident Management, Reporting & Co. S. 26
- Internet Services, Apps & Co. S. 28
- Cyber Security S. 30
- Social Media – Fake-Profiles S. 32
- Desinformation, Fake News & Co. S. 34
- Security @work - tägliche Fallstricke S. 36
- Security @home S. 38
- Connected Car Security S. 40
- Digital Parcours – Future Jobs S. 36
- Compliance Parcours (10 Stationen) www.known-sense.de/ComplianceParcoursKatalog.pdf

Aktuell in Planung sind weitere Stationen, z. B.:

- Sicherheit in der Cloud
- Verschlüsselung
- CEO-Fraud
- Außerdem weitere Themenstationen für unseren neuen Digital Parcours

Die Preise der Security Arena

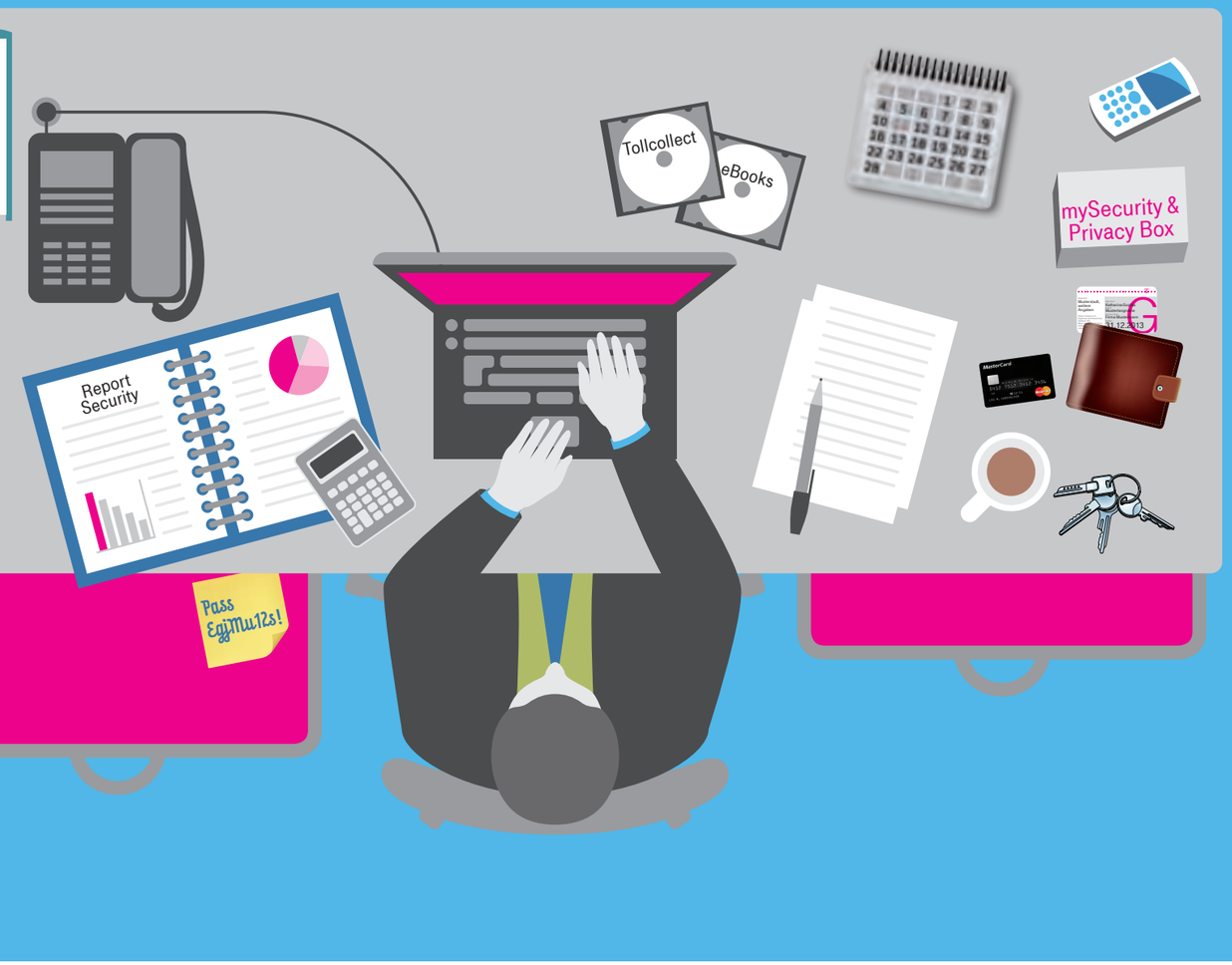
Normalerweise lizenzieren wir das Format an unsere Kunden im Train-the-Trainer-Verfahren, d. h. Sie führen Security Arenen eigenständig mit Ihren Mitarbeitern als Moderatoren durch. Hierfür fordern Sie bitte unsere Preisliste via sense@known-sense.de an. Sie können jedoch auch über uns Moderatoren buchen und stellen dann für Events nur Raum und Teilnehmer – den Rest übernehmen wir. Unser Berechnungsmodell dafür finden Sie im Kasten auf der rechten Seite.

Weitere Informationen: www.known-sense.de/2017_known_sense_Awarenessflyer.pdf

Security Arena – Awareness Circle-Training ‚out of the box' (Überblick)	
Zielgruppe(n)	▸▸ Alle Mitarbeiter, ▸▸ Spezifische Zielgruppen: Sonder-Arenen für Manager, IT-Admins, HR, Rezeptionisten etc. möglich
Content (Auswahl)	▸▸ Alles auf Deutsch/Englisch verfügbar – weitere Sprachen möglich ▸▸ Kunde sucht sich Stationen aus ▸▸ Incentivierung empfohlen (inkl. Preise für Siegerteam)
Optionaler Medien-einsatz	▸▸ Ausdehnung bzw. Verdichtung durch Event-Add-Ons wie Security. Marktplatz, World Café, begehbare Riesenspiele, Videos, Vorträge etc.
Ziele (Auswahl)	▸▸ Sicherheitsthemen werden durch den diskursiven Team-Ansatz in einen produktiven Umsatz gebracht ▸▸ Spielerischer Ansatz schafft hohes Invovement und verbindet Sicherheit mit positiven Erlebnissen (Emotion steigert Memorierbarkeit) ▸▸ Setting sichert hohe Visibility und adressiert die Intensivierung diverser Memo-Techniken ▸▸ Als Teaser für vertiefende Maßnahmen oder Kampagnen-Launch ▸▸ Gewinnung von Sicherheits-Vorbilder bzw. -Botschaftern
Teilnehmer-zahl, Preise & Optionen bei Moderation durch known_ sense	▸▸ Berechnungsgrundlage und Preise bei einmaligen Events mithilfe unserer Moderatoren: ▸▸ 1 Trainings-Run = 60 (4 Stationen) oder 90 Minuten (6 Stationen ▸▸ Bis zu 6 Stationen pro Event-Tag möglich mit z. B. ▸▸ bis 20 TN ab 900,00 Euro netto zzgl. Reisekosten ▸▸ bis 35 TN ab 1.300,00 Euro netto zzgl. Reisekosten ▸▸ bis 70 TN ab 1.800,00 Euro netto zzgl. Reisekosten ▸▸ bis 140 TN ab 3.200 Euro netto zzgl. Reisekosten ▸▸ bis 280 TN ab 5.400 Euro netto zzgl. Reisekosten ▸▸ **Alle Materialien können auch lizenziert und über unseren Train-the-trainer-Ansatz eigenständig in Organisationen implementiert werden.**

DATENSCHUTZ

Datenschutz	
Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. HR
Content (Auswahl)	▸▸ Welche Daten speichern wir über Sie? ▸▸ Für welche Zwecke speichern und nutzen wir diese Daten? ▸▸ Welche Rechte haben Sie bezüglich Ihrer persönlichen Daten? ▸▸ Wie lange speichern wir Ihre Daten? ▸▸ Wen können Sie bei Fragen zu persönlichen Daten kontaktieren?
Ressourcen	▸▸ 1 Riesenpuzzle (Acryl), 100 x 70 cm, 45 „richtige" und 9 „falsche" Teile ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung) ▸▸ Optional (Spiel 2): DIN-lang-Spielkarten
Spielmechanik	▸▸ Spiel 1: Die Teilnehmer setzen Antworten auf 5 Fragen zum Thema Mitarbeiter-Datenschutz aus Puzzleteilen mit Textfragmenten zusammen. Die Texte sind auf einzelnen Körperteilen einer Mitarbeiterfigur aufgedruckt. Es passen nur die Teile mit den „richtigen" Antworten in das Puzzle (Spieldauer 5 Min.) ▸▸ Optional (Spiel 2): Ein Domino mit ca. 14 Textfragmenten aus Merksätzen zum Thema Datenschutz ▸▸ Reine Spieldauer jeweils 2 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer erfahren Grundlagen des Datenschutzes, indem sie reflektieren, was über sie selber durch Ihr Unternehmen gesammelt und gespeichert wird und welche grundsätzlichen Rechte mit personenbezogenen Daten verbunden sind.



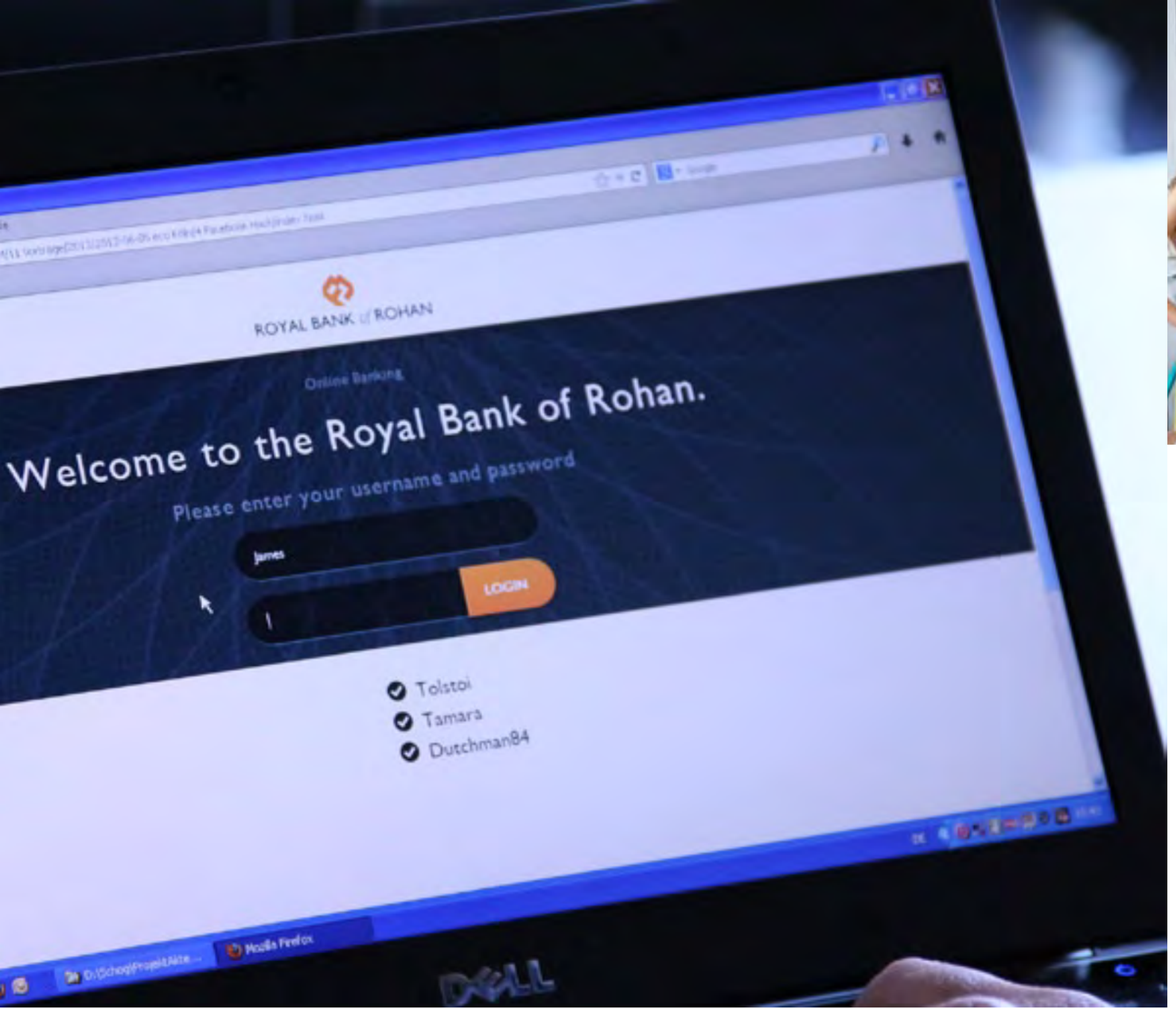
CLEAR DESK

Clear Desk/Clean Desk

Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ „Aufgeräumter" Arbeitsplatz aus Sicht des Prinzips Clear bzw. Clean Desk ▸▸ Szenarien: Arbeitsplatz, Büro/Großraumbüro, Meeting-Raum etc.
Ressourcen	▸▸ 1 grüne und 1 rote Filzdecke ▸▸ 25 Dokumente und Gegenstände zum Sortieren – Objekte müssen vom Anwender gestellt werden (optional Objekte auf Spielkarten verfügbar) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren 25 typische Objekte, die sich an einem Arbeitsplatz befinden könnten, entsprechend ihrer Sensitivität in „liegen lassen" bzw. „einschließen". ▸▸ Reine Spieldauer 2 Min.
Ziele (Auswahl)	▸▸ Vermittlung der Clear bzw. Clean Desk-Policy als eines der Schlüsselprinzipien der Informationssicherheit

INFORMATIONS-KLASSIFIZIERUNG

Informations-Klassifizierung	
Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Unterschied von Daten und Informationen ▸▸ Klassifikationsprinzipien ▸▸ Merkmale der verwendeten Klassen ▸▸ Kennzeichnen, Übertragen und Entsorgen
Ressourcen	▸▸ 25 laminierte Dokumente bzw. Stellvertreter für Dokumente (Cover o. ä.) – Dokumente müssen vom Anwender gestellt werden ▸▸ 3-4 farbige Filzdecken mit Displays zum Sortieren ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung) ▸▸ ggf. als Add-on Informations-Drehscheibe zur Demonstration des Klassifizierens (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren 25 typische Dokumente die sich an einem Arbeitsplatz befinden könnten, entsprechend ihrer Sensitivität in 3-4 Klassen ▸▸ Reine Spieldauer 2 Min.
Ziele (Auswahl)	▸▸ Vermittlung der Information Classification-Policy mit den entsprechenden Klassen als Hauptprinzip der Gewährleistung von Informationssicherheit



PASSWORD HACKING

Password Hacking	
Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Access Protection als wichtiges Prinzip der Informationssicherheit ▸▸ Bilden eines starkes Passworts ▸▸ Eselsbrücken und andere Memotechniken zum Merken von Passwörtern ▸▸ Erstellen von Deep Information Cluster via Social Media
Ressourcen	▸▸ Hacking Software ▸▸ ca. 5 Hardcopies von Social Media-Profilen (wird auf Basis einer möglichen Kampagnen-Leitfigur des Anwender erstellt – optional: Standardprofil wird gestellt) ▸▸ Moderations-Briefing ▸▸ 1 Notebook für die Installation der Hacking Software ▸▸ Optional: 1- 2 Beamer zum Übertragen von Notebook-Monitor und/ oder Profil ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sollen mithilfe von Informationen eines Social-Media-Profils und einem Notebook einen virtuellen Account („Zamaon" oder „Bank of Rohan") hacken ▸▸ Reine Spieldauer 5 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, wie einfach triviale Passwörter zu identifizieren sind, wenn über die Zielperson private Informationen, z. B. via Social Media, verfügbar sind

Sicherheits-Parcours

Station Besucher und Ausweise

BESUCHER & AUSWEISE

Besucher & Ausweise

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Rezeptionisten
Content (Auswahl)	▸▸ Zutrittsprozesse bzw. -kontrolle ▸▸ Verschiedene Berechtigungen und Ausweise ▸▸ Verhalten beim Antreffen von „Fremden" bzw. Personen ohne Ausweis in den eigenen Liegenschaften
Ressourcen	▸▸ Spielfeld ▸▸ Spielkarten ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung) ▸▸ Optional (Spiel 2): 1-3 Riesenpuzzles mit div. Ausweisen
Spielmechanik	▸▸ Die Teilnehmer visualisieren mithilfe eines Spielfeldes und verschiedener Karten den Zutrittsprozess diverser Mitarbeiter,, Lieferanten, Partner und Gäste zu verschiedenen Organisationsbereichen bzw. Räumen ▸▸ Optional (Spiel 2): Die Teilnehmer legen Riesenpuzzles verschiedener Ausweise (z. B. Mitarbeiter, Gast) zusammen ▸▸ Reine Spieldauer 2-6 Min. (je nach Tiefung)
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, wie sie mit Besuchern bzw. potenziell unberechtigten Personen umgehen sollen

Social Media	
Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. HR
Content (Auswahl)	▸▸ Welchen Content (Bild, Text) darf ich in Social Media unter meinem Unternehmens-Account veröffentlichen? ▸▸ Datenschutz in Social Media ▸▸ Cyber-Mobbing ▸▸ Social Engineering in sozialen Netzwerken
Ressourcen	▸▸ 1 grüne und 1 rote Filzdecke ▸▸ 24 Spielkarten (DIN A6) ▸▸ 16-20 Moderationskarten ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren 8 Fotos (als Warming-up) und 16 potenzielle Statusmeldungen aus Social Media , die sich auf Karten befinden, auf einer grünen bzw. roten Decke in „erlaubt" und „nicht erlaubt" ▸▸ Reine Spieldauer 3 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer reflektieren ihre eigenen Aktivitäten und Erfahrungen in Social Media und setzen diese in Bezug zu den Sicherheitsinteressen ihrer Organisation durch den Abgleich mit den offiziellen Social Media-Guidelines

SOCIAL MEDIA

Security Arena: **Social Engineering**

Social Engineering

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Manager, Rezeptionisten, Office-MA
Content (Auswahl)	▸▸ Social Engineering – Begriff und Einordnung in ein Big Picture von Cyber Crime & Co. ▸▸ CEO-Fraud ▸▸ Soziale Einfalltore ▸▸ Kommunikationskanäle von Face-to-face bis zur E-Mail ▸▸ Diverse Kommunikationslayer (verbal, nonverbal, paraverbal) ▸▸ Intuition bzw. Bauchgefühl ▸▸ Opfer-Täter-Beziehung ▸▸ Schuid und Scham und SE Incident Management
Ressourcen	▸▸ Spielfeld (ca. DIN A1) ▸▸ 16 Spielkarten (DIN A6) ▸▸ Moderations-Briefing ▸▸ Social-Engineering-Wheel ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung) ▸▸ auf Wunsch als Add-ons SE-Selbsttest „Bluff-O-Meter“ bzw. Riesenspiel „Bluff & Hack“ (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer ordnen 16 potenzielle Zitate von Social Engineers, die sich auf Karten befinden, auf einem Spielfeld den entsprechenden sozialen Einfalltoren zu. ▸▸ Reine Spieldauer 3 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, dass es SE gibt, was sich dahinter verbirgt, mit welchen Methoden die Angreifer operieren und was diese Methoden mit den eigenen kommunikativen bzw. sozialen Stärken und Schwächen zu tun haben

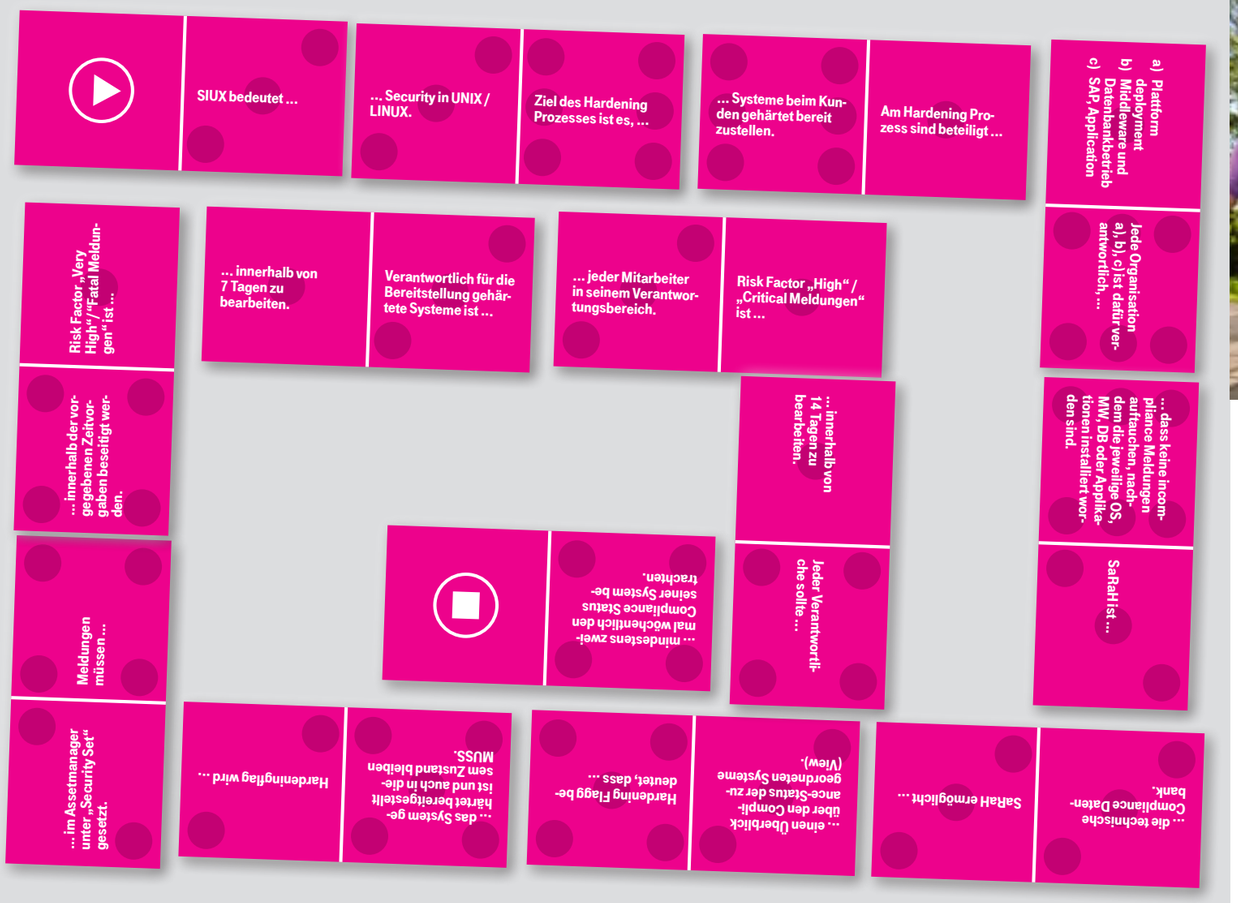
SOCIAL ENGINEERING

PHISHING

Phishing	
Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Arten von Phishingmails ▸▸ Klassen von Phishing-Merkmalen ▸▸ Beurteilung von E-Mails auf Basis von Checklisten und Prozesse ▸▸ Reporting bzw. Incident Management bei Phishing – privat und in der Organisation ▸▸ Big Picture Social Enginnering u. a. Manipulationen ▸▸ Ransomware & Co.
Ressourcen	▸▸ 1 grüne und 1 rote Filzdecke ▸▸ faltbares Display (offen 120 x 50 cm) ▸▸ 2 Spielangelnmit Ringmagneten ▸▸ mind. 15 Spielkarten (DIN B5) ▸▸ magnetische Metallclips ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer angeln aus einem Karten-Display mithilfe von Magnetangeln E.Mails, die sie in „Phishing" bzw. „kein Phishing" sortieren sollen. ▸▸ Reine Spieldauer 3 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen die unterschiedlichen Merkmale potenzieller Hinweise auf Phishingmails kennen und was man idealerweise unternimmt, wenn man doch einmal reingefallen ist

Sicher unterwegs

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. MA mit hoher Reisetätigkeit
Content (Auswahl)	▸▸ Travel Security – wie verhalte ich mich auf Reisen ▸▸ Verschiedene Szenarien und Lokationen: Flughafen (Wartebereich, Security etc.), Anfahrt (Taxi, ÖPNV etc.), Hotel, Meetingräume etc. ▸▸ Richtige Vorbereitung und Vorsichtsmaßnahmen, richtiges Reagieren
Ressourcen	▸▸ Spielfeld (ca. 170 x 120 cm) ▸▸ je 14 rote und grüne Spielkarten (DIN B7) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren auf einer Lernkarte (Wimmelbild), die die Umgebung eines Flughafen zeigt, 14 Risiko- und 14 Defense-Karten zu den jeweils passenden Situationen der Abbildung. ▸▸ Reine Spieldauer 2 mal 2:30 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, mit welche Informationssicherheitsrisiken man beim Reisen konfrontiert wird und mit welchen Maßnahmen man diese mindern kann



Sichere Server

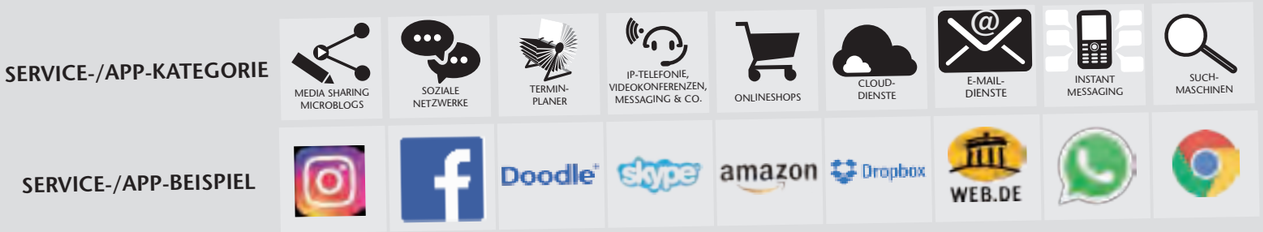
Zielgruppe(n)	▸▸ MA der IT
Content (Auswahl)	▸▸ Hardening als „Key“ bei der Plattformsicherheit ▸▸ Plan – build – run! ▸▸ SIUX – UNIX – LINUX
Ressourcen	▸▸ 18 Spielkarten (DIN lang) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung) ▸▸ Optional (Spiel 2): Netzwerkpuzzle
Spielmechanik	▸▸ Die Teilnehmer setzen Bezeichnungen bzw. Fragmente eines Textes zum Thema Hardening (optional Netzwerke) auf Basis von Dominokarten (optional Magnetfolien) zusammen ▸▸ Reine Spieldauer ab 3 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen den Hardening-Prozess im Kontext des Aufbaus von sicheren Servern (optional die Struktur eines typischen Netzwerkes) kennen

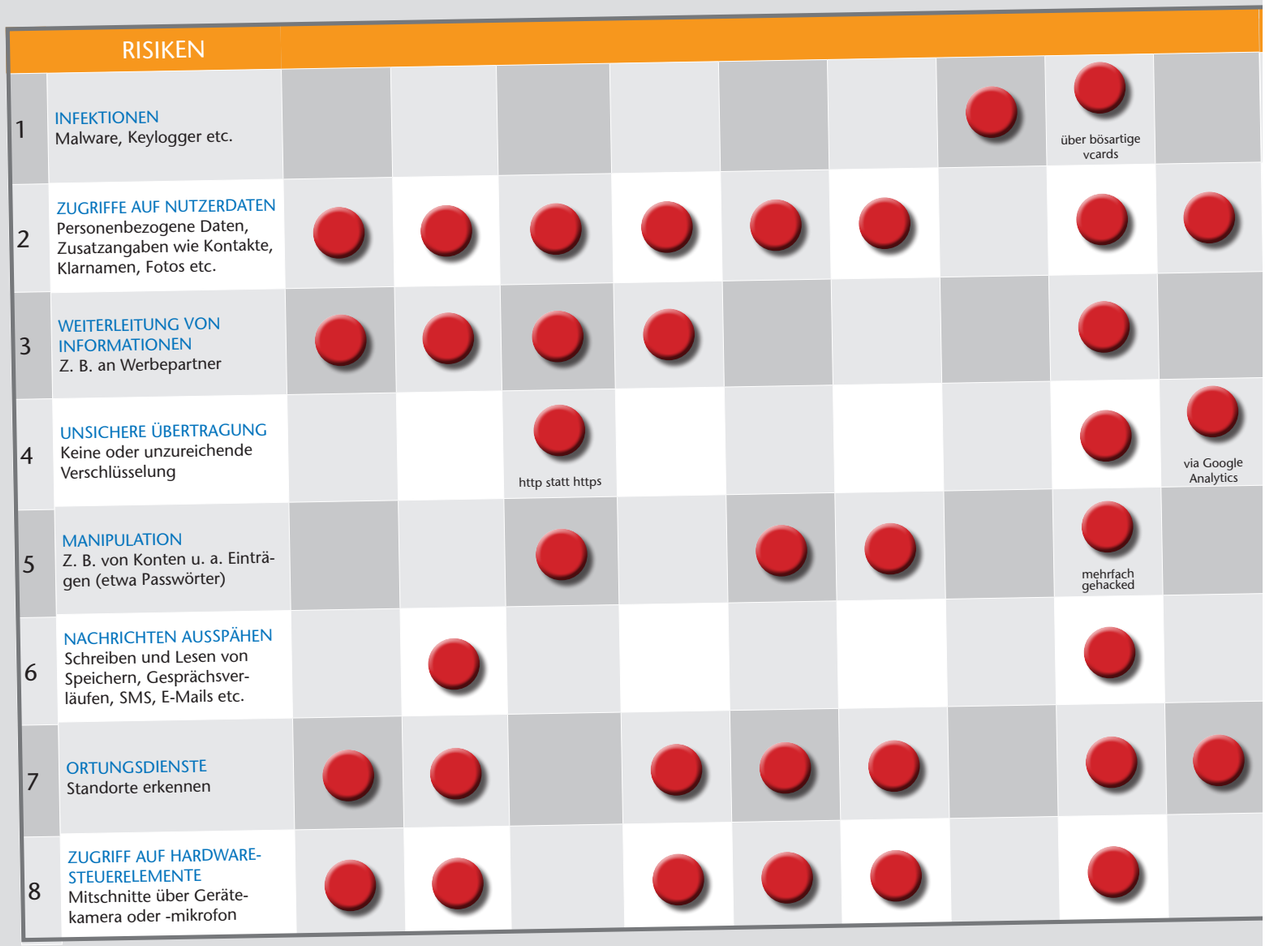
SICHERE SERVER

Incident Management, Reporting & Co.

Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Kontakte ▸▸ Incident vs. „kein Incident“ – Definitionen und persönliche Erfahrungen ▸▸ Eskalation und Behandlung ▸▸ Themen: IT, Hinweigebersysteme, Privacy, Compliance etc. ▸▸ Fehlverhalten ▸▸ Voraussetzungen für Meldungen ▸▸ Was muss geschützt werden?
Ressourcen	▸▸ Spielfeld (ca. 80 x 80 cm) ▸▸ 12 Spielkarten (DIN A6) mit Szenarien als Story ▸▸ farbige Jetons ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ 12 verschiedene Security-Fälle sind als Minigeschichte auf Karten abgedruckt, die die Teilnehmer auf dem Spielfeld entlang der passenden Icons richtig sortieren sollen. Anschließend sollen farbige Jetons, die stellvertretend für verschiedene Reporting-Einfalltore stehen, passend zugeordnet werden ▸▸ Reine Spieldauer 5 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, was unter Security Incidents verstanden wird und was ggf. nicht. Außerdem die richtigen Meldestellen für Security (Privacy, Compliance, etc.), dass man nicht „falsch“ melden kann, dass aber ein zielgenaues Rporting den Support Zyklus kürzer gestaltet

INTERNET SERVICES, APPS





INTERNET SERVICES, APPS & CO.

SecurityArena

Projekt: SecAware4job

Internet Services, Apps & Co.

Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Nichts ist umsonst – wir bezahlen mit unseren „guten" Daten ▸▸ Welche Internet Services bzw. Apps nutzen wir regelmäßig und welche Zugriffe erlauben wir diesen? ▸▸ Sind diese Zugriffe notwendig, um den Service bzw. die App produktiv zu nutzen und wen nicht, wie kann ich die abstellen? ▸▸ Gibt es in meiner Organisation sichere Alternativen?
Ressourcen	▸▸ Spielfeld (ca. 80 x 80 cm) ▸▸ 9 Spielkarten mit Logos ▸▸ ca. 30 farbige Jetons ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sollen auf einem Spielfeld mit 9 Apps bzw. Internet Services (z. B. WhatsApp oder Google Translate) und 8 Risiko-Cluster jeweils dort rote Jetons platzieren, wo sie in Bezug auf die App bzw. den Service ein Datenschutzrisiko vermuten ▸▸ Reine Spieldauer 4 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, hinter welchen Kategorien bzw. populären, konkreten Beispielen von Internet Services bzw. Apps Datenschutzrisiken – wenn nicht klar identifiziert – zumindest vermutet werden können und erhalten über die zu bildende Matrix ein einprägsames Big Picture

Cyber Security

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Manager, Vorstände, MA aus Financial & Control
Content (Auswahl)	▸▸ Welche Fälle von Cyber Crime sind bekannt mit welchen – vor allem finanziellen – Auswirkungen? ▸▸ Was kostet ein Cyber-Vorfall und welche konkreten Positionen sind daran beteiligt?
Ressourcen	▸▸ 10 Spielkarten (DIN A4) mit der Kurzbeschreibung konkreter Fälle von Incidents, Fraud bzw. Hacks & Co. ▸▸ Cyber-Money (mit bekannten Hackern und Whistleblowern) – 6 verschiedene Werte ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer erhalten bis zu 10 DIN-A4-Sheets mit Profilen populärer Cyber Incidents (Ransomware, CEO-Fraud, gehackte Nutzerdaten etc.) und einen Stapel Spielgeld. Das Spielgeld soll in einer Höhe auf die Fallkarten abgelegt werden, so dass sie die geschätzten Kosten, die der jeweilige Fall verursacht hat, entsprechen ▸▸ Reine Spieldauer 6 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen unterschiedliche Ansätze von Cyber Crime kennen und welche konkreten Kosten damit verbunden sind

Social Media – Fake Profile

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. HR
Content (Auswahl)	▸▸ Woran erkenne ich gefälschte Profile? Was sind typische Standardkategorien und Prozesse, auf die ich bei meiner Beurteilung setzen sollte? ▸▸ Intuition bzw. Bauchgefühl ▸▸ Welche Motive treibt die Absender? Was ist das Big Picture hinter Fake Profilen? ▸▸ Social Engineering und Deepfake? ▸▸ Konkrete persönliche Erfahrungen
Ressourcen	▸▸ 1 grüne und 1 rote Filzdecke ▸▸ 20 Spielkarten (DIN A4) mit realen oder gefälschten Social Media-Profilen ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren 20 Social Media-Profile auf eine grüne (real) oder rote Decke (Fake) ▸▸ Reine Spieldauer 5 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, auf ganz bestimmte Hinweise bei der Beurteilung von Social Media-Profilen zu achten und ggf. auch ihrer Intuition zu trauen

DESINFORMATION, FAKE NEWS & CO.

Desinformation, Fake News & Co.

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Manager und MA der Kommunikation
Content (Auswahl)	▸▸ Geschichte von Desinformation und Big Picture im Kontext Manipulation ▸▸ Trolling ▸▸ Warum sind Fake News auch als Informationssicherheitsrisiko zu betrachten? ▸▸ Auf welche Details habe ich bei der Beurteilung von Informationen zu achten? Was sind Hinweise für Fake News? ▸▸ Meldungen als Geschichte sowie deren emotionale Anteile ▸▸ Spezieller Umgang mit Fotos und Bildsuchmaschinen
Ressourcen	▸▸ 15 grüne und 15 rote Karten zum Abstimmen ▸▸ 16 Spielkarten (DIN A6) mit realen oder gefälschten Meldungen ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sollen 16 Meldungen, die Ihnen vorgelegt werden, mit einer grünen (real) oder roten Karte (fake) kommentieren – die mehrheit innerhalb des teams entscheidet. ▸▸ Reine Spieldauer 4 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, Meldungen zu beurteilen und welche spezifischen Merkmale auf Fake News hindeuten. Außerdem, wie Sie hiölfreiche Recherche-Tools nutzen, um Informationen zu beurteilen und warum Desinformation grundsätzlich ein Risiko für Unternehmen darstellt.

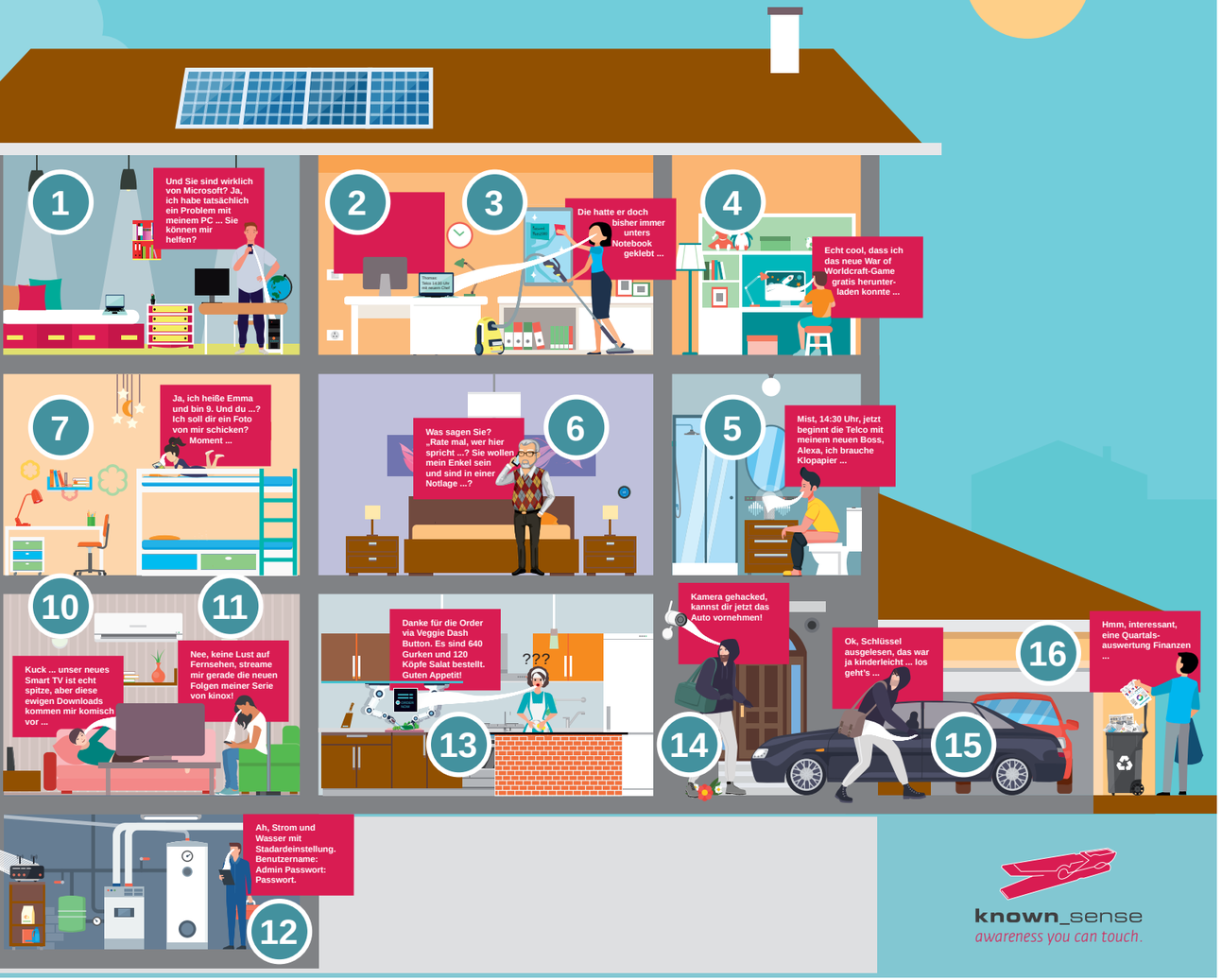
SECURITY @WORK

Security@work – tägliche Fallstricke auf der Arbeit

Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Rezeptionisten
Content (Auswahl)	▸▸ Clean Desk ▸▸ Amok, Terror u. a. Bedrohungen am Arbeitsplatz ▸▸ Social Engineering via Telefon bzw. face-to-face ▸▸ Dumpster Diving ▸▸ Sicheres Drucken ▸▸ Sichere Entsorgung ▸▸ Informations-Klassifizierung ▸▸ E-Mail-Security, Phishing & Co. ▸▸ Passwort-Security ▸▸ Access Protection
Ressourcen	▸▸ Spielfeld (ca. 120 x 170 cm) ▸▸ je 14 rote Risikokarten und 14 grüne Defense-Karten (DIN B7) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren auf einer Lernkarte (Wimmelbild), die eine typische Arbeitsumgbung im Büro zeigt, 14 Risiko- und 14 Defense-Karten zu den jeweils passenden Situationen der Abbildung ▸▸ Reine Spieldauer 2 mal 2:30 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, mit welche Informationssicherheitsrisiken man auf der Arbeit konfrontiert wird und mit welchen Maßnahmen man diese mindern kann

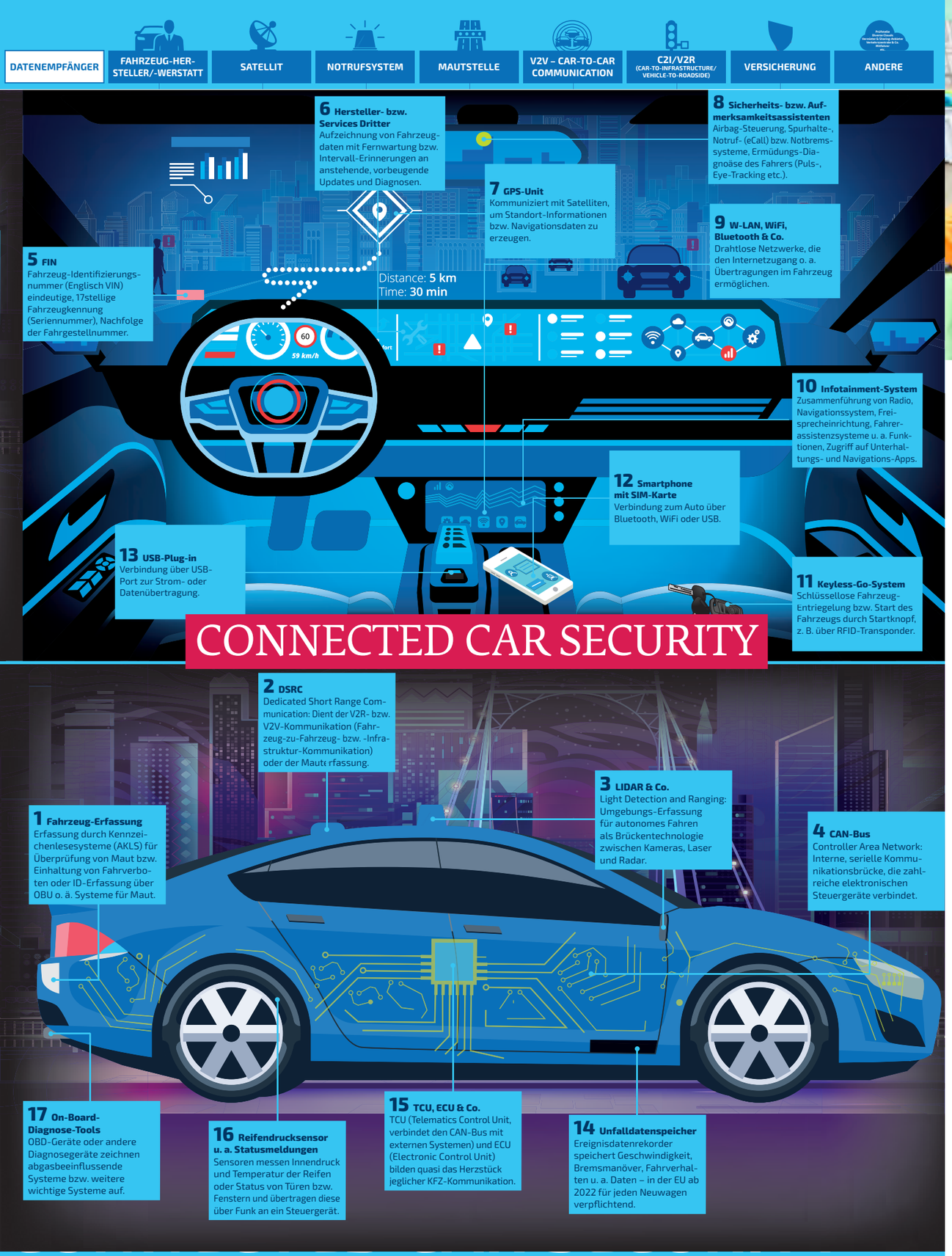
SECURITY @HOME

SECURITY ARENA: Security@home



known_sense
awareness you can touch.

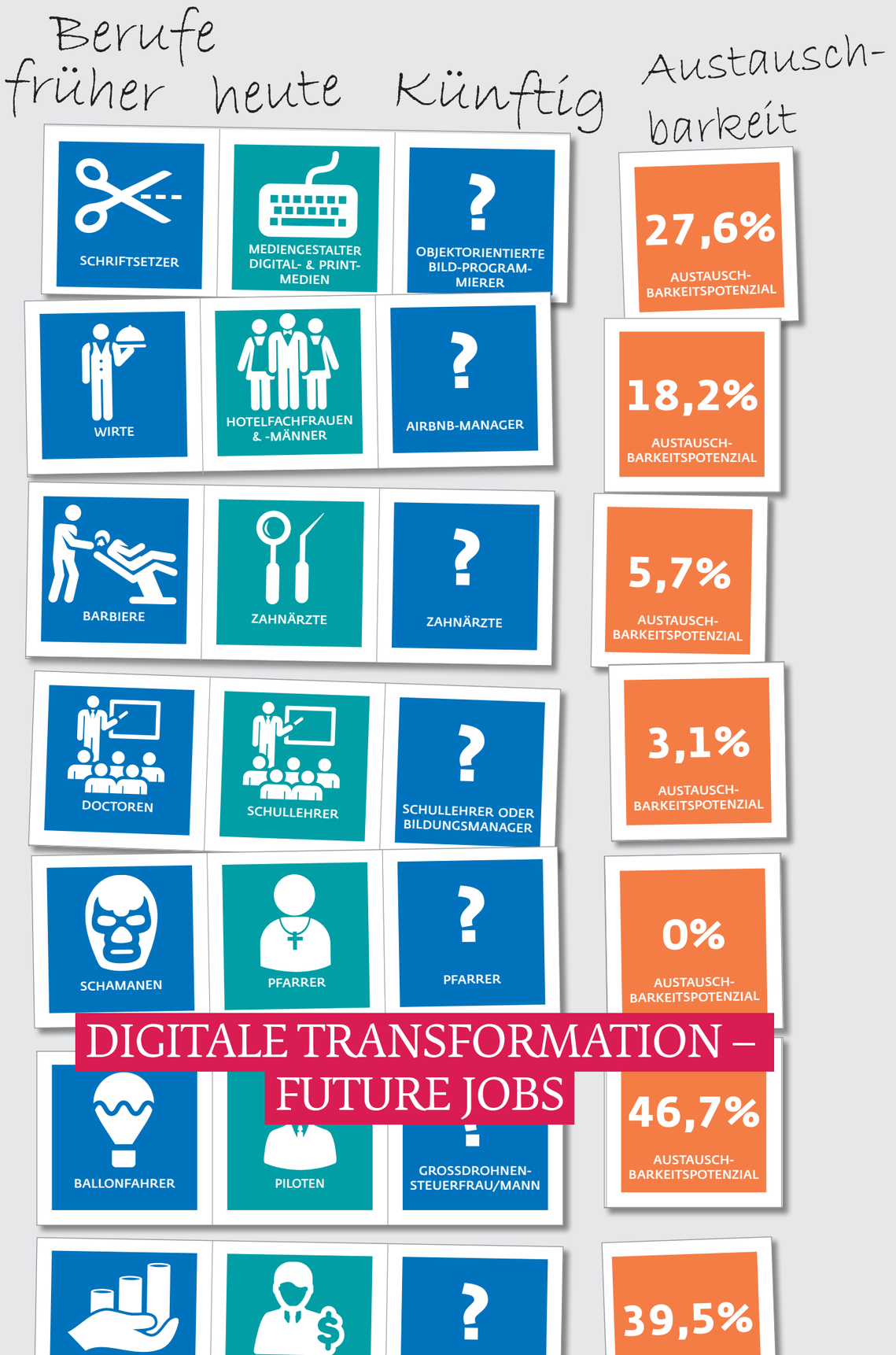
Security @home	
Zielgruppe(n)	▸▸ alle Mitarbeiter, insbes. Mitarbeiter im Home Office
Content (Auswahl)	▸▸ Clean Desk ▸▸ Social Engineering, Telefonbetrug, Support-Abzocke & Co. ▸▸ Dumpster Diving ▸▸ E-Mail-Security, Phishing & Co. ▸▸ Passwort-Security ▸▸ Illegale Downloads, illegales Streaming ▸▸ Smart TV ▸▸ Sprachbasierte Systeme ▸▸ Telcos & Video-Konferenzen ▸▸ Cyber Grooming ▸▸ Mithören bzw. Ausspionieren ▸▸ Überwachungskameras ▸▸ Unsicheres WLAN ▸▸ Smart Home, smart Grid ▸▸ Keyless Go-Systeme
Ressourcen	▸▸ Spielfeld (ca. 120 x 170 cm) ▸▸ je 15 rote Risikokarten und 15 grüne Defense-Karten (DIN B7) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren auf einer Lernkarte (Wimmelbild), die eine typisches Einfamilienhaus mit Home Office zeigt, 15 Risiko- und 15 Defense-Karten zu den jeweils passenden Situationen der Abbildung ▸▸ Reine Spieldauer 2 mal 2:30 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, mit welche Sicherheitsrisiken Mitarbeiter im Home Office und deren Familien zuhause konfrontiert sind und mit welchen Maßnahmen man diese mindern kann



Connected Car Security

Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Backdoors, Malware & Co. ▸▸ Manipulation ▸▸ Bilderkennung bzw. Kennzeichen-Erfassung ▸▸ Spoofing ▸▸ Tracking ▸▸ Datenerfassung, -übertragung und -verarbeitung ▸▸ Diebstahl ▸▸ Zugriffsrechte ▸▸ Hijacking, Hacks & Co.
Ressourcen	▸▸ Spielfeld (ca. 120 x 170 cm) ▸▸ je 17 rote Risikokarten und 17 grüne Defense-Karten (DIN B7) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sortieren auf einer Lernkarte (Wimmelbild), die zwei Perspektiven eines typischen, vernetzten Autos zeigt, 17 Risiko- und 17 Defense-Karten zu den jeweils passenden Situationen der Abbildung ▸▸ Reine Spieldauer 6 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, mit welche Sicherheitsrisiken sie in ihren Connected Cars konfrontiert sind und mit welchen Maßnahmen man diese mindern kann

Digital Parcours Station „Futurejobs" by known_sense (Auszug)



Digitale Transformation – Future Jobs

Zielgruppe(n)	▸▸ alle Mitarbeiter
Content (Auswahl)	▸▸ Welche heutigen Jobs könnten infolge der Digitalisierung potenziell ersetzt werden und mit welchem Austauschbarkeitspotenzial? ▸▸ Ist das Verschwinden von Berufen bzw. Profilen bereits aus der Geschichte bekannt? D.h. welche früheren Jobs sind durch aktuelle ersetzt worden? ▸▸ Muss ich befürchten, dass auch mein Jobprofil auf der Kippe steht? ▸▸ Was bedeutet überhaupt Digitalisierung und welche Chancen ergeben sich aus der digitalen Transformation für mein Unternehmen und mich persönlich?
Ressourcen	▸▸ 48 Spielkarten (ca. 7 x 7 cm) ▸▸ Moderations-Briefing ▸▸ auf Wunsch Poster und/oder Aufsteller (gehört nicht zur Standardausstattung)
Spielmechanik	▸▸ Die Teilnehmer sollen eine Reihung von 48 Karten vornehmen für 12 verschiedene, typische Berufsprofile früher – heute - zukünftig plus das jeweilige Austauschbarkeitspotenzial schätzen ▸▸ Reine Spieldauer 5 Min.
Ziele (Auswahl)	▸▸ Die Teilnehmer lernen, dass die digitale Transformation neben Risiken vor allem auch Chancen für ihr Unternehmen und sie persönlich birgt und welche Profile dabei potenziell gebraucht werden bzw. welche ggf. weniger. Über den gemeinsamen Diskurs und den historischen Blick zurück werden ihnen die Bedenken im Kontext Digitalisierung als reiner Vernichter von Arbeitsplätzen genommen

LÄNDER, IN DENEN KNOWN_SENSE AWARENESS-PROJEKTE DURCHGEFÜHRT HAT

Unsere Kampagnen wurden in 46 Ländern in insgesamt 25 Sprachen ausgerollt. Als Manager von und Trainer für gamifizierte Security Awareness-Events bzw. -Roadshows haben wir in 16 Ländern auf allen 5 Kontinenten gearbeitet.

Sprachen, in denen die Arena verfügbar ist:

Komplett: Deutsch/Englisch
In Auszügen:
- Bulgarisch
- Chinesisch
- Französich
- Griechisch
- Italienisch
- Kroatisch
- Polnisch
- Portugisisch
- Rumänisch
- Russisch
- Slowakisch
- Spanisch

SECURITY ARENA ANWENDER

- Allianz (SE und Group)
- Amadeus
- BAköV
- Berliner Wasserbetriebe
- BMW Group
- Bundesnetzagentur
- Bundesrat
- Bürgschaftsbank NRW
- Bürkert
- Commerzbank
- DB Systel
- Deutsche Bahn
- Deutsche Telekom
- DIHK
- DSE Europe
- EnBW
- E.ON
- EulerHermes
- EVLKA
- FIZ – Forschungszentrum Informatik
- Gruner und Jahr
- IWC SChaffhausen (CH)
- Kärcher
- Munich Re
- Open Grid Europe
- Physikalisch-Technische Bundesanstalt
- RISCS – Research Institute in Science of Cyber Sec (UK)
- RWE
- Santander Bank
- SIX Group
- Stiftung Alsterdorf
- Swiss Post (CH)
- TH Wildau
- T-Systems International
- Uniper
- Volkswagen
- Wesley Mission Queensland (AUS)
- Wirecard

BRANDING UND LIZENZEN

Die jeweils aktuelle Preisliste für die Nutzung im Train-the-trainer-Verfahren mit Branding und inhaltlichen Anpassungen an Ihre Organisation erhalten Sie via Anfrage über sense@kown-sense.de.

- Geliefert wird ab 4 Stationen ein handelsüblicher Hartschalenkoffer mit allen notwendigen Materialien in gelabelten Kunststoffboxen zzgl. sämtlicher Daten in digitaler Form (jedoch keine offenen Dateien).
- Ab 4 Stationen mit bis zu 8 halbstündige Telcos zur Begleitung der Anpassung, Methoden-Inkubation, Beratung und (innerhalb Deutschlands) eine bis zu 3-stündigen Train-the-trainer-Session (zzgl. Reisekosten) inkludiert.
- Der Titel „Security Arena" kann wahlweise übernommen oder individuell angepasst werden.
- In Addition dazu Verfügbarkeit von zusätzlichen Eventmaterialien wie Checklisten, Workflow- und Organisationshilfen (Templates für Zeitplan, To-do-Listen, Punktezettel, Giveaway- und Incentive-Katalog, Teilnehmer-Zertifikat, Teilnehmerrechner sowie Promotion-Templates wie E-Mail-Einladungen, Artikelmodule, No-Photo-Button – Poster, Flyer, Aufsteller optional gegen Aufpreis).
- Zusätzliche Leistungen (z. B. Illustrations-Adaptionen, weiteres Train-the-Trainer der Moderatoren, Co-Organisation bzw. Supervision von Trainings und Events, Zertifizierung von Moderatoren, individuelle Medien-Anpassungen, Übersetzungen sowie Logistikkosten (Versand u.ä.) und u. U. notwendige Reisekosten bei Beratungen on Location werden extra nach Aufwand zu einem Tagessatz von netto € 1.300,00 abgerechnet.
- Bei Vertragsabschluss ist ein Pflichtenheft inkludiert.
- Preise für Leihstationen zur einmaligen Nutzung – optional inklusive Moderation durch known_sense s. S. 5.

Haben Sie Fragen zu den Stationen, zum Lizenzmodell oder Branding bzw. anderen Adaptionen? Melden Sie sich bitte bei uns:

known_sense | Jakob-Engels-Straße 39 | 51143 Köln
Fon +49 2203 1831618 (Ansprechpartner Dietmar Pokoyski)
E-Mail und Web: sense@known-sense.de bzw. www.known-sense.de

TEILNEHMER-MEINUNGEN

„Ich habe nach der Arena sofort meine Passwörter geändert".

„Das macht Spaß und ist lehrreich, alle mussten die ganze Zeit über grinsen – diese Arena sollte verpflichend für alle sein."

„Danke für diesen geilen Tag!"

"The event was very educational, fun, and challenging as it required us to think and act urgently, with caution and working with a group of individuals who are unique. It was wonderful."

"Well presented. Presentors were warm, smiling, make feel you at home, friendly."

"I would recommend this to all employees, so make it compulsory to attend."

"I feel it's easier to learn when having fun, and this event provided exactly that. It was a great initiative that surely has, and will continue to, yield great regards in as far as security awareness is concerned. Big ups!"