Fraunhofer IAO

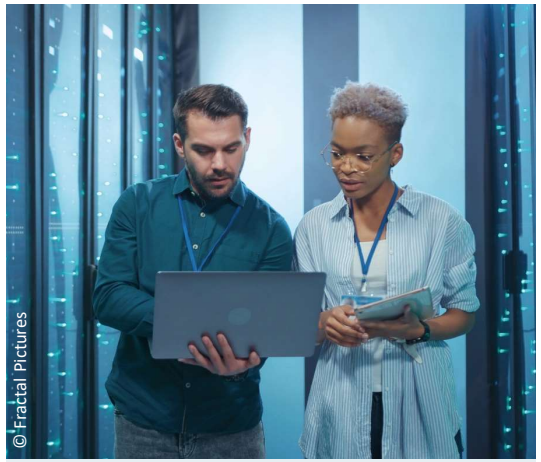
HOCHSCHULE HEILBRONN

Dr. Heiko Roßnagel, it-sa Nürnberg, 22.10.2024

»Der Faktor Mensch in der IT-Sicherheit«

Unsere Themen

Wirtschaftliche, positiv erlebbare und organisatorisch tragfähige Cybersicherheit



IT-Sicherheitsrisiken managen
Unser datengetriebener Ansatz ermöglicht Risiken schlank, schnell und verständlich zu managen. So wird IT-Sicherheit planbar.

Sicherheitsfaktor Mensch
IT-Sicherheit erlebbar machen, Social-Engineering vorbeugen und erfolgreiches Security Policy Management macht aus Ihren Beschäftigten Ihre besten Verteidiger.

Identity Management
Von Produktion bis Bürger, Vertrauenslisten bis hoheitliche Identitäten, Blockchain bis Directory Service. Wir entwickeln moderne und pragmatische Lösungen.

Konstruktiver Datenschutz
Datenschutz darf nicht bremsen. Mit unserer Expertise ermöglichen wir Compliance unter Wahrung funktionaler Anforderungen.

Der Faktor Mensch

a.k.a „The User“

„Nutzer sind dumm und faul“

„Sie interessieren sich nicht für Sicherheit“

„Sie umgehen regelmäßig Sicherheitsrichtlinien“

„Klicken auf alles was sich bewegt“

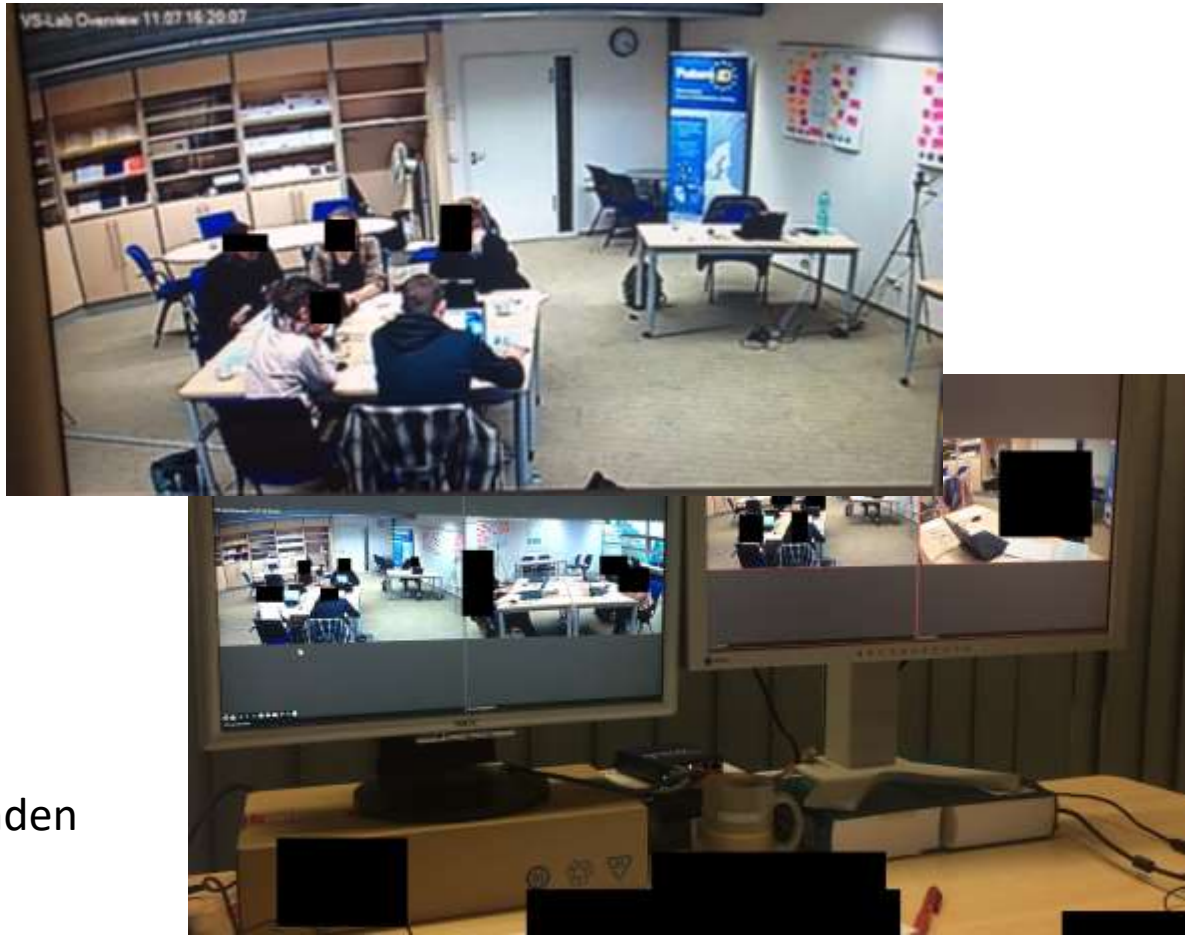
Annahmen:

- Nutzer sind nicht von sich aus motiviert, sich sicher zu verhalten
- Ein sicheres Verhalten kann durch Übungen und Androhung von Strafen im Falle der Nichteinhaltung erreicht werden

Der soziale Einfluss von IT-Sicherheit

Ein Experiment zum Umgang mit Sicherheitsmechanismen unter Stress

- Experiment zu Policy Compliance
  - Fiktives Engineering Setting mit Sicherheits-Maßnahme und Sicherheitsrichtlinie
  - Simulierter Druck durch 3 fiktive Kunden über 2 Tage

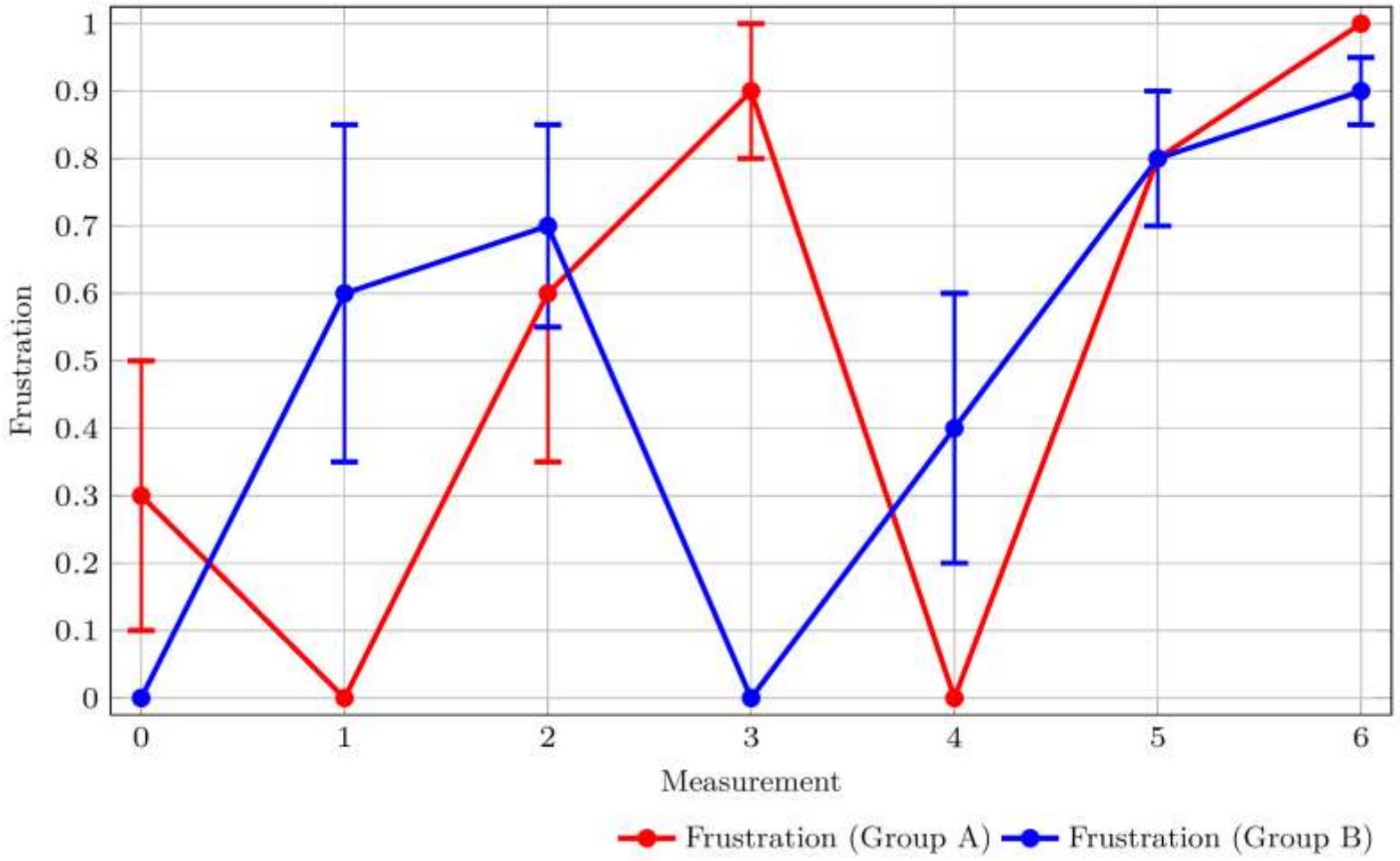


- Positive Haltung zur Umsetzung der Sicherheitsrichtlinie beobachtbar:
  - Unabhängig von Charaktereigenschaften
  - Bis der Druck zu groß wurde
  - Sicherheitsmaßnahme wird als Behinderung empfunden
  - Dies führt zu nachhaltigem Policy Bruch

Kurowski, Sebastian; Fähnrich, Nicolas; Roßnagel, Heiko (2018): On the possible impact of security technology design on policy adherent user behavior - Results from a controlled empirical experiment. SICHERHEIT 2018. DOI: 10.18420/sicherheit2018_11. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-675-6. pp. 145-158. Wissenschaftliche Beiträge. Konstanz, Germany. 25.-27. April 2018.

Der Soziale Einfluss der IT-Sicherheit

Mitarbeiter, die Sicherheitsmaßnahmen als Behinderung empfinden, stellen eine Schwachstelle dar.



HOCHSCHULE HEILBRONN

Fraunhofer IAO

Was können wir aus diesem Experiment lernen?

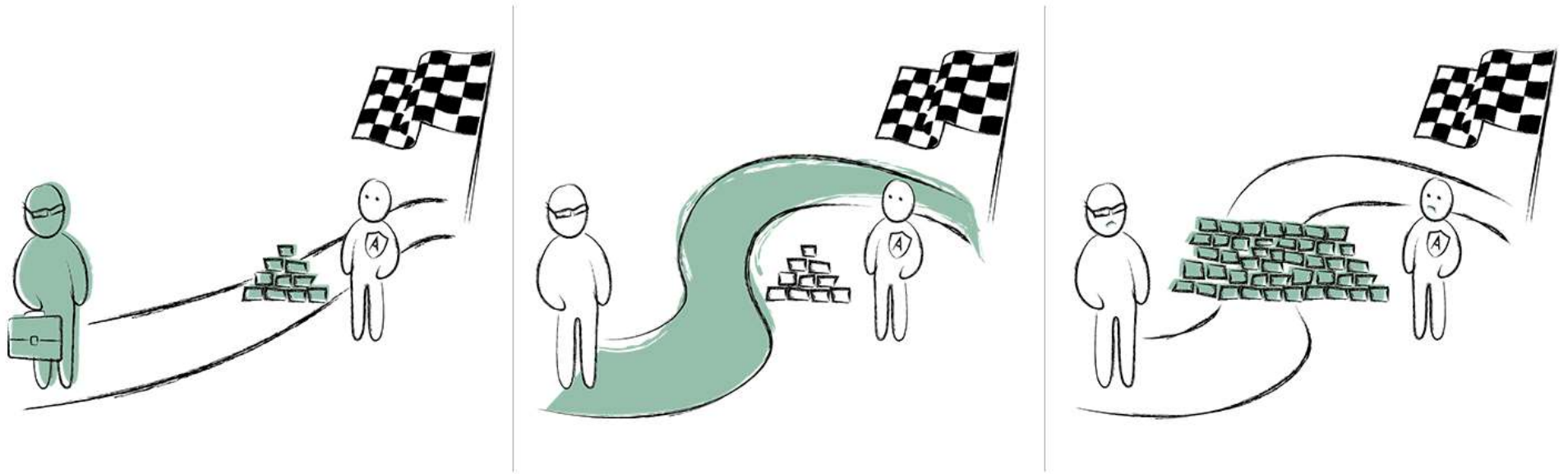
- Awareness ist nicht genug. Es ist nur der erste Schritt zu sicherem Verhalten.
- Die Risikowahrnehmung verschiedener Personen kann sehr unterschiedlich sein.
- Es gibt viel Gründe, warum sich Nutzer nicht so sicher verhalten wie gewünscht.
- Es ist nicht immer der Fehler der Nutzer.

Offene Interessenskonflikte

Abteilungen arbeiten gegeneinander statt miteinander

Interessenskonflikte: ehrgeizigen Zielvorgaben, Zeitdruck und dem Interesse an guter Zusammenarbeit mit KollegInnen stehen oftmals abstrakte IT-Sicherheitsrisiken und -vorschriften gegenüber.

Dies führt regelmäßig zu Konflikten innerhalb des Unternehmens z.B. zwischen IT und Fachabteilung.

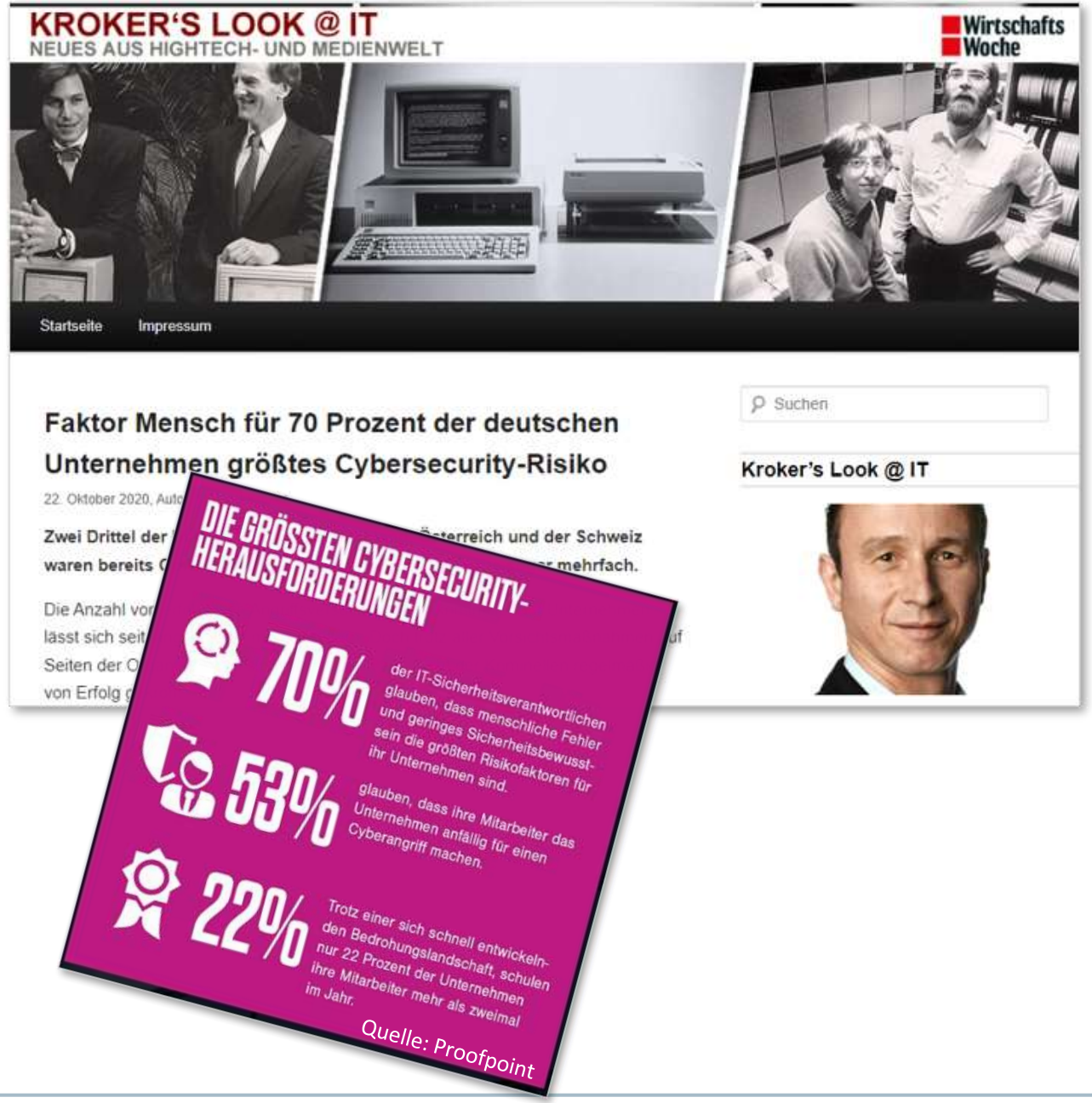


Lernlabor Cybersecurity
»Sicherheitsfaktor Mensch«

Vision

1. Das Lernlabor »Sicherheitsfaktor Mensch« wird zu Deutschlands führendem Lernort und Kompetenzzentrum für den »Faktor Mensch« in der IT-Sicherheit.

2. Entwicklung von Konzepten und Lernangeboten, für die nachweislich demonstriert ist, dass sie mit dem »Faktor Mensch« verbundene Sicherheitsrisiken signifikant reduzieren.



HOCHSCHULE HEILBRONN Fraunhofer IAO

Inhaltlicher Schwerpunkt
»Sicherheitsfaktor Mensch«

Zielsetzung

1. Aktuelle Forschungsergebnisse zum Themenschwerpunkt »Sicherheitsfaktor Mensch«, praxisnah und anwendungs-orientiert in Wirtschaft und Gesellschaft bringen.

2. Schaffung eines innovativen Lernorts zur Deckung des Qualifizierungsbedarfs von Fach- und Führungskräften, in dem IT-Sicherheit mit Fokus auf den »Faktor Mensch« erlebbar wird.

3. Einbeziehung breiter Bevölkerungsschichten von jung bis alt, um die gesamtgesellschaftliche Dimensionen des »Sicherheitsfaktor Mensch« zu adressieren.

Forschungsschwerpunkte

Strategische Ausrichtung des Lernlabors

1. **Verhaltensorientierte Forschung im Bereich IT-Sicherheit**
   Unter Verwendung von empirischen Methoden untersuchen wir, wie sich Menschen im Bereich IT-Sicherheit verhalten. Wir ermitteln die Ursachen und Gründe für ihre Verhaltensweisen und untersuchen, wie diese positiv beeinflusst werden können.

2. **Menschengerechte Gestaltung von IT-Sicherheitstechnologien, -richtlinien und -maßnahmen**
   Wir untersuchen, wie man IT-Sicherheit so gestalten kann, dass sie eine positive User Experience erzeugt, Marktbedürfnisse erfüllt und Nutzeranforderungen gerecht wird. Aufbauend auf empirischen Erkenntnissen, werden interdisziplinäre Methoden eingesetzt und entwickelt, um eine menschengerechte Gestaltung zu ermöglichen

3. **Entwicklung neuer zielgruppengerechter Lehr- und Lernformate**
   Es werden Lehr- und Lernformate entwickelt, die eine aktive Beteiligung der Lernenden ermöglichen, praktische Versuche und Erlebnisse umfassen, um Grundprinzipen und Verständnis der Thematik und Theorie zu fördern. Darauf aufbauend werden Kompetenzen zur praktischen Lösung von Problemen vermittelt, sowie kritisches Denken und Reflektion und die Problemlösungsfähigkeiten der Lernenden gefördert.

Forschungsschwerpunkte

Strategische Ausrichtung des Lernlabors

4. **Stärkung von Kompetenzaufbau und nachhaltiger Verhaltensänderung in Unternehmen**
   Es wird erforscht welche Veränderungen in IT und Prozessen in Unternehmen erforderlich sind, um eine nachhaltige *Verhaltensänderung* von Miterarbeitenden zu unterstützen und wie dies optimal mit Weiterbildungen verbunden werden kann. Dazu gehört eine Verzahnung von externer Weiterbildung mit Lernschritten im Unternehmenskontext für die Umsetzung des Gelernten in sichere Routinen. Dafür werden wissenschaftliche Erkenntnisse bzw. Expert*innen zu Verhaltensänderung mit einbezogen.

5. **Entwicklung von Evaluationsmetriken**
   Wir erforschen, wie sich der Erfolg von neuen Lehr- und Lernformen nachweisen und messen lässt. Das Ziel ist es nachweislich zu demonstrieren, dass die entwickelten Konzepte und Lernangebote in der Lage sind, mit dem »Faktor Mensch« verbundene Sicherheitsrisiken signifikant reduzieren. Dies erfolgt in enger Abstimmung mit der Fraunhofer Academy, um die gewonnenen Erkenntnis in die Gesamtevaluation der Lernlabore einfließen zu lassen.

Herkömmliche Schulungsansätze

- **Aufklärungskampagnen:** Was darf man tun und was nicht?
- **Seminare** mit reiner Theorie ohne Praxisanteil
- **Online-Kurse**, die häufig nur „durchgeklickt“ werden
- Vorführung von Angriffen im Rahmen von **Live-Hacking-Demos** ohne aktive Beteiligung der Teilnehmenden

- → **eingeschränkte Wissensvermittlung**
- → die **Teilnehmenden** erfahren mehr über IT-Sicherheit, sind aber meist **für den Ernstfall nicht vorbereitet.**

Erleben statt predigen

Cyberangriffe selbst ausprobieren

- **Erleben** von verschiedenen **Cyberangriffen:**
  - Phishing/Spear-Phishing
  - Ransomware
  - USB-Angriffe
  - Man-in-the-Middle-Angriffe
- **Immersiver Erlebnisort** für IT-Sicherheit
- **Fokus** auf dem **Faktor Mensch**
- **Immersiven Erlebnisatmosphäre** zur Abbildung von **KMU-typischen Arbeitsplätzen** mit entsprechender Hard- und Software

Weiterbildungsangebote zum „Faktor Mensch in der IT-Sicherheit“

Maßgeschneidert für die Bedürfnisse Ihres Unternehmens

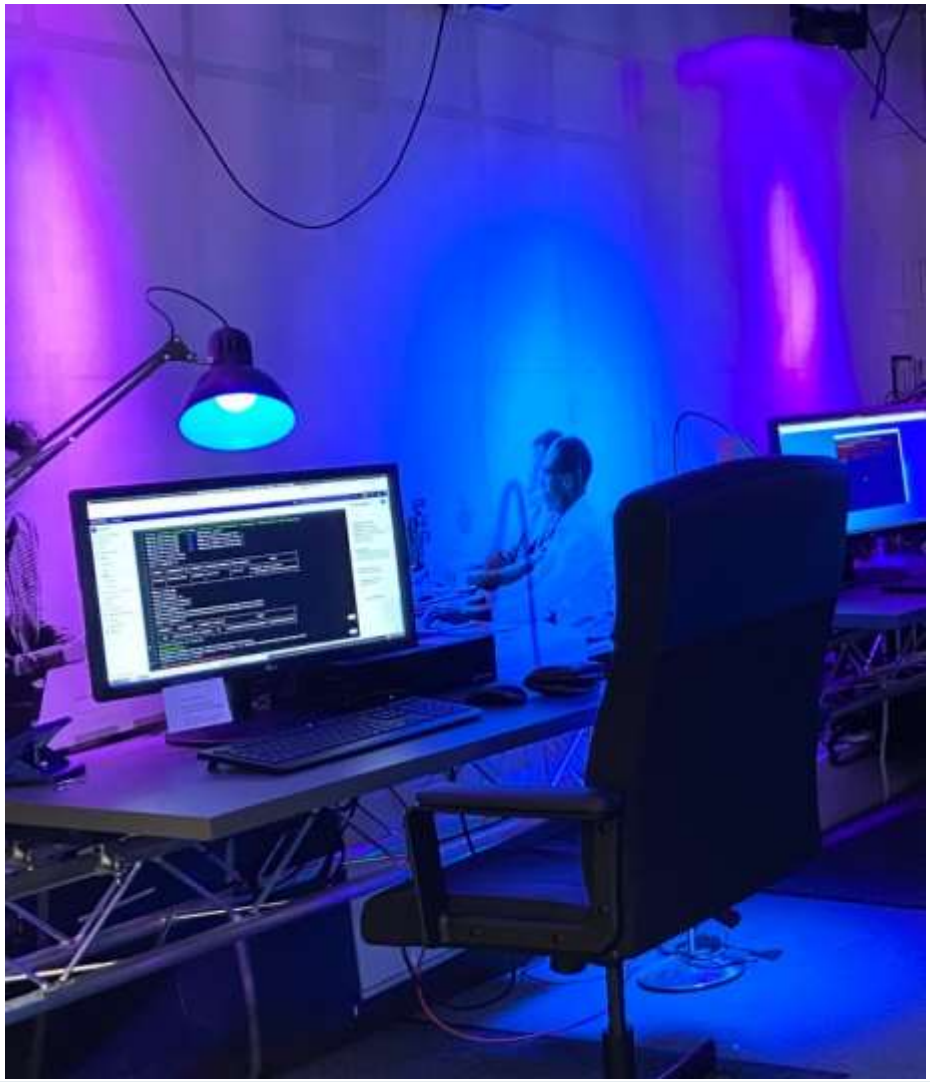
Modularer, zielgruppenspezifischer Aufbau

Fokus auf die für die Zielgruppe relevanten Themen

Praxisbezug zum konkreten Arbeitsalltag der Zielgruppe

Erlebnisorientiert und interaktiv

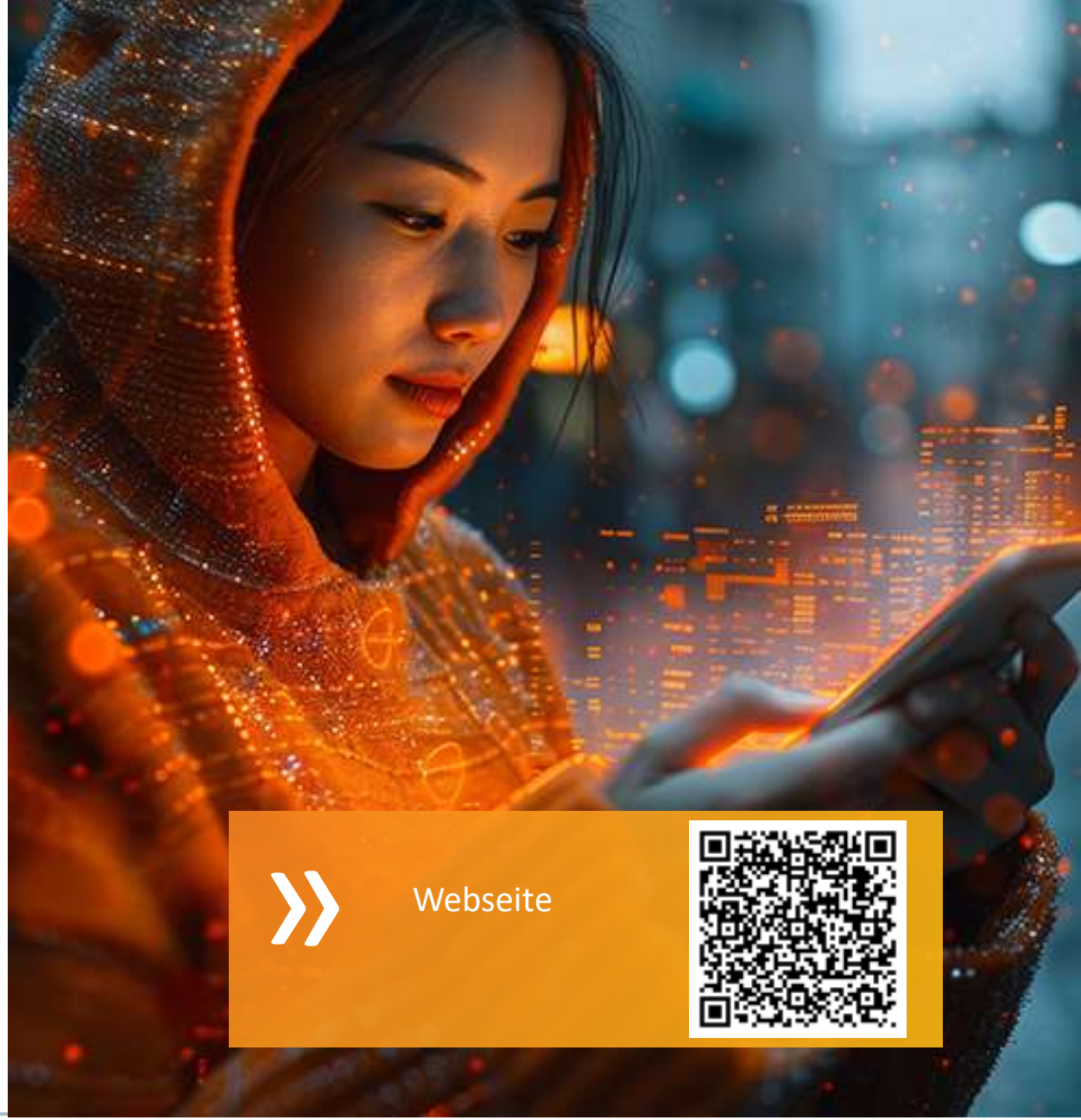
Verständlich auch ohne IT oder Cybersicherheitshintergrund



Lernlabor Cybersicherheit

Schwerpunkt: Faktor Mensch

- Bildungscampus Hochschule Heilbronn, Gebaude 17, Raum S0.21
- Interaktive Demonstratoren, um verschiedene Formen von Cyberangriffen zu erleben
- Online-/Offline-Schulungen mit dem Schwerpunkt Mensch und Cybersicherheit
  - Schutz vor CEO- und Finanzbetrug
  - Empathisches Sicherheits-Policy-Engineering
  - Konfliktlösende Sicherheitskommunikation



Vielen Dank für Ihre Aufmerksamkeit

Dr. Heiko Roßnagel

Team Identitätsmanagement

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

heiko.rossnagel@iao.fraunhofer.de

+49 711 970 2145