ALARM
Awareness Labor KMU
Informationssicherheit

Gemeinsam zum **Projekterfolg**

Neue Wege für mehr
Informationssicherheit in KMU

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Mehr Einblicke in unserem Projektvideo!

alarm.wildau.biz

IMPRESSUM

Herausgeberin
Prof. Dr. Margit Scholl
Technische Hochschule Wildau
Hochschulring 1
15745 Wildau
alarm@th-wildau.de
Autor und Autorinnen
Hubertus v. Tippelskirch
Frauke Prott
Margit Scholl
Gestaltung
Olesja Mujkic und
Forschungsgruppe Scholl
Bilder
Falls nicht entsprechend mit Quellen anders vermerkt, Bildnachweis:
© Forschungsgruppe Scholl
Titelgrafik: Forschungsgruppe Scholl

September 2023

ISBN 978-3-949639-07-4

INHALT

KONZEPT

SECHS GEMEINSAME ERFOLGSGESCHICHTEN

Über zwanzig Jahre Erfahrung und eine mit vielfältigen Projektpartnerinnen und -partnern verwirklichte Vision

© RBB24 Brandenburg Aktuell, 30.11.2022

„In den vergangenen Jahren wurde in der betrieblichen Sicherheitsforschung immer deutlicher, dass die Menschen in den Unternehmen einen wichtigen Faktor zur Steigerung des Sicherheitsniveaus darstellen.“

Prof. Dr. Margit Scholl, Projektmanagement, Technische Hochschule Wildau (TH Wildau)

Informationssicherheit durch die Projektergebnisse in Ihrem Unternehmen erhöhen

Die Ergebnisse des „Awareness Labors KMU (ALARM) Informationssicherheit“ bieten einen in der betrieblichen Praxis erprobten Beitrag zu der dringend notwendigen Sensibilisierung für Informationssicherheit von Führungskräften und Mitarbeitenden und damit zur Stärkung von Informationssicherheitsbewusstsein (Information Security Awareness). Sie können mit den Projektergebnissen eine gezielte Personalentwicklung in Ihrem Unternehmen etablieren, Sicherheitsthemen konkret (be-)greifbar machen und Ihre Mitarbeitenden erlebnisorientiert sensibilisieren sowie weitergehend schulen. Beziehen Sie Ihre Mitarbeitenden aktiv in die Nutzung dieser Sensibilisierungsmaßnahmen ein und bauen Sie so eine nachhaltige Informationssicherheitskultur auf. Streben Sie für Ihr Unternehmen eine Zertifizierung nach ISO/IEC 27001 an, so können diese Maßnahmen gleichzeitig als Nachweise für die geforderte Kompetenzentwicklung dienen.

Angebot direkt online und unentgeltlich erhältlich

Ihnen stehen unter anderem sieben digitale und analoge Serious Games zur Verfügung. Die digitalen Versionen können direkt genutzt werden. Für die Durchführung analoger Awareness- und Schulungsmaßnahmen in Ihren Unternehmen liegen Anleitungen für die Moderation und alle benötigten Materialien als Download bereit. Handlungsempfehlungen aus ausgewerteten „Vor-Ort-Angriffen“ und ein Wissensselbsttest befähigen Sie, selbstständig IT-sicherheitsrelevante Entscheidungen zu treffen. Reports, tiefenpsychologische Studien und internationale Publikationen geben Ihnen weitergehende Denkansätze. Die Verzahnung dieser Werkzeuge bietet Ihnen einen starken Antrieb, um den Herausforderungen einer wachsenden Cyber-Bedrohungslage erfolgreich zu begegnen. Das Angebot ist kostenfrei für die interne, nicht-kommerzielle Nutzung.

Die sechs Erfolgsgeschichten dieses dritten Reports berichten von gemeinsamen Eindrücken, Hürden, Lösungswegen und Errungenschaften des Projekts. Verantwortliche sowie Interessierte in KMU, Interessensverbänden, IT-Dienstleistungsunternehmen, Politik und Forschung sind eingeladen, unsere Erfahrungen als Anregungen für die eigene betriebliche Umsetzung der Materialien zu nutzen.

Analoge Serious Games fördern Awareness Trainings

„Das Thema rückte zunächst natürlich in den Vordergrund und war Gesprächsthema. Die Sensibilisierung ließ dann allerdings – erwartungsgemäß – nach, sodass erneute Trainings nötig wurden, um das Awareness-Level hoch zu halten.“

Frank Bader, Chief Financial Officer, division one

MISSION:
Einbettung der Informationssicherheit in den Arbeitsalltag

Im Projekt wurde iterativ in drei Phasen agil und partizipatorisch ein innovatives Gesamtszenario für Informationssicherheit entwickelt und unter Beteiligung von Pilot-KMU erprobt. Die erlebnisorientierten analogen Serious Games sind ein wichtiger Bestandteil davon. Mit Moderationsanleitungen ausgestattet ist jede für Informationssicherheit zuständige Person in der Lage, die Moderation zu übernehmen. Die analogen Serious Games dienen als wertvolle Lernstationen mit skalierbarer Spieldauer, sodass sie von 15 Minuten bis zu einer Stunde Diskussion und Training bieten. Sie können sowohl zur Erinnerung und Verfestigung als auch für neue Mitarbeitende zum Einstieg genutzt werden. Als Workshop angeboten sind sie wichtiger Bestandteil eines Awareness Trainings, das auch zur Einschätzung der Informationssicherheitskultur genutzt werden kann.

PARTNERINNEN UND PARTNER
Pilotunternehmen
Mitarbeitende und Studierenden der TH Wildau
known_sense (Entwicklung)

KOOPERATION
Testung, Messung und Evaluation

SCHWERPUNKT
Sensibilisierung in der Praxis
Anwendungsnahe Forschung
Enger Austausch und Hilfestellung

Übergabe des Awareness-Koffers durch die Projektleitung als Dank an Frank Bader.

Awareness Training am analogen Serious Game „Homeoffice“ in den Räumlichkeiten des Stuttgarter Pilotunternehmens. Vier Mitarbeitende in einer Diskussion über ihre unterschiedlichen Technikaffinitäten.

HERAUSFORDERUNG

KMU mangelt es oft an den notwendigen Ressourcen für Informationssicherheit. Heterogenität der Belegschaft, geringe Awareness-Reife und häufig verschwimmende Aufgabenbereiche in KMU erfordern eine breite Vermittlung von Grundlagen. Sensibilisierungsmaßnahmen müssen zeitlich und inhaltlich skalierbar sein, um dem unterschiedlichen Awareness-Reifegrad der KMU gerecht und im Tagesgeschäft etabliert werden zu können. Besonders in Zeiten von Pandemie und geopolitischen Umwälzungen sollte notfalls eine hybride Nutzbarkeit über Videokonferenzsysteme möglich sein.

DURCHFÜHRUNG

In den Jahren 2021 und 2022 wurden zwei Awareness Trainings im Stuttgarter Pilotunternehmen und an der TH Wildau eines mit einem Pilotunternehmen aus der Region und ein weiteres mit Studierenden in Teilgruppen von drei bis vier Personen durchgeführt. Terminabsprachen für die Trainings wurden mit besonderer Rücksicht getroffen. Je nach Pandemielage wurde das Hygienekonzept angepasst. Vor und nach der Testung wurden die analogen Serious Games anonymisiert evaluiert und durch ein Beobachtungsprotokoll beurteilt.

ERFOLG

Die Inhalte der analogen Serious Games wurden mehrheitlich als wichtig eingestuft und lösten lebhafte Diskussionen aus. Einzelheiten in den Lernszenarien, wie unklare Begriffe oder zu lang empfundene Texte auf Karten, wurden anhand der Evaluation verbessert. Wiederkehrende Kritik an den Lernszenarien betraf die zu knappe Zeit für wertvolle Diskussionen. Die Evaluation ergab unter anderem, dass Teilnehmende eine merkliche Steigerung des Sicherheitsgefühls wahrnahmen. Im Ergebnis konnten sieben analoge Serious Games, trotz Pandemie, erfolgreich entwickelt und erprobt werden.

Moderationsausbildung schafft Multiplikatorinnen und Multiplikatoren

„Wer gerne spielt (Karten- oder Gesellschaftsspiele), der erkennt sofort den Spielmechanismus und kann ihn auch leicht an die Mitspieler weitergeben. ... Man kommt schnell mit den Teilnehmern zu IT- Sicherheitsthemen ins Gespräch und man merkt, dass man mit diesen Problemen nicht alleine ist.“

Jens Jankowsky, Referent für Innovation/Energie, IHK Ostbrandenburg

MISSION:

Schaffung von Reichweite und Verständnis für Methoden und Ansätze

Im Projekt kam es zum Wissensaustausch und gemeinsamen Entwicklungen mit Forschungsprojekten, Institutionen und Studierenden. Ein Schwerpunkt lag auf einer starken Präsenz durch Beiträge in wissenschaftlichen Veröffentlichungen, auf Konferenzen, Messen und eigenen Awareness Foren. Im Mittelpunkt standen dabei Einblicke in die praktische Anwendbarkeit, Vermittlung der Lernmethoden und die Selbstbefähigung. Wichtige Multiplikatorinnen und Multiplikatoren bilden Forschungseinrichtungen, öffentliche Transferstellen, staatliche Anlaufstellen und Kompetenzzentren im Mittelstand. Von Beginn an standen Interessensverbände wie Industrie- und Handelskammern (IHK) eng an der Seite des Projekts.

Teilnehmende einer Moderationsausbildung im Januar 2023 bei einer Problemlösungsaufgabe durch kreatives Denken und Gestalten.

PARTNERINNEN UND PARTNER
Pilotunternehmen
Assoziierte Partnerinnen und Partner wie IHK und HWK
Kompetenzzentren und Bildungseinrichtungen

KOOPERATION
Erhalt und Zertifizierung einer Fortbildung

SCHWERPUNKT
Sensibilisierung in der Praxis
Hilfe zur Selbsthilfe
Vernetzung und Verbreitung

Übergabe des Awareness-Koffers durch die Projektleitung als Dank an Jens Jankowsky.

HERAUSFORDERUNG

Die entwickelten Methoden entfalten erst ihre ganze Stärke, wenn sie in ein umfassendes Trainingskonzept integriert werden. Sicherheitskonzepte müssen kommuniziert, digitale Serious Games durch eine fortlaufend aktive Moderation gerahmt und besonders analoge Serious Games anregend und flüssig angeleitet werden. Schriftliche Moderationsanleitungen versetzen zwar Anwendende in die Lage, Serious Games zu nutzen, eine Professionalisierung bedarf aber tiefergehender Techniken.

DURCHFÜHRUNG

Im November 2021 wurden innerhalb eines internen Kreativ-Workshops von known_sense und der Forschungsgruppe gemeinsam innovative Spielprinzipien, Spielpsychologie und Moderationstechniken vertieft. Im Mai 2022 und Januar 2023 wurde das Moderationskonzept auf die entwickelten Serious Games angewandt und an der TH Wildau Moderationsausbildungen angeboten. Gegenstand waren Moderationstechniken, Aufwärm- und Vertiefungsübungen und Anwendungsbeispiele für Stationenlernen.

ERFOLG

Durch die Moderationsausbildung wurden die Teilnehmenden staatlicher Transferstellen, der Digitalagentur Berlin, der Universität Potsdam, der Humboldt Universität zu Berlin, des Zukunftszentrums Brandenburgs, der Handwerkskammer (HWK) Potsdam, der IHK Ostbrandenburg und weiterer Bildungseinrichtungen in die Lage versetzt, eigene Workshops zu führen, die Lernmethoden des Projekts anzuwenden und zu verbreiten. Der Austausch von Expertisen aus Didaktik und der Praxis ließ alle profitierten.

Entwicklerinnen und Entwickler digitaler Serious Games profitieren mehrfach

„Natürlich spielt Cyber Security für uns als Games Unternehmen im Alltag eine zentrale operative Rolle. Es ist jedoch nochmal etwas anderes, diese Inhalte als ein Lernerlebnis aufzubereiten. Hier haben wir den Austausch mit den anderen Unterauftragnehmenden und der TH Wildau als sehr bereichernd und fruchtbar erlebt. … Wir nutzen die digitalen Lernszenarien nun selbst … im Onboarding neuer Teammitglieder genauso wie im regelmäßigen Auffrischen der Inhalte.“

Ulrike Küchler, Geschäftsführung, Gamebook Studio

MISSION:

Regelmäßige Sensibilisierung zur Steigerung des Informationssicherheitsbewusstseins

Serious Games bieten in der Nachbildung realistischer Alltagssituationen einen geschützten Raum, in dem Fehler gemacht, Konsequenzen von getroffenen Entscheidungen ohne Folgen für das wahre Leben erlebt und verschiedene Wege ausprobiert werden können. Narratives Lernen mit digitalen Serious Games zum Thema Informationssicherheit wird positiv angenommen und trägt zum Lernerfolg bei. Typische Gefahrensituationen, Realitätsnähe, sowohl Überblick als auch gezielte Vertiefung und vielseitige Integration in firmeneigene Trainingskonzepte werden von einer motivierenden Geschichte getragen.

Ausschnitt aus dem Vortrag „Sensibilisierung für Informationssicherheit durch Storytelling am Arbeitsplatz: Digitale Lernszenarien“ von Ulrike Küchler, Gamebook Studio beim Awareness Forum 2023 des Projekts (© Gamebook Studio).

PARTNERINNEN UND PARTNER

Pilotunternehmen
Studierende der TH Wildau
Gamebook Studio (Entwicklung)

KOOPERATION

Testung, Messung und Evaluation

SCHWERPUNKT

Sensibilisierung in der Praxis
Anwendungsnahe Forschung
Hohe Reichweite und Alltagsintegration

Übergabe des Awareness-Koffers durch die Projektleitung als Dank an Ulrike Küchler.

HERAUSFORDERUNG

Im Gegensatz zu analogen Serious Games erfolgen digitale meist unbegleitet, wodurch Nutzende stärker durch eine gute Geschichte, ansprechendes Design, Belohnungen und geschmeidigen Fluss im Szenario gehalten werden müssen. Klärung offener Fragen erfolgt nicht aktiv moderiert, sondern in Eigenregie. Spezialisierte Spielentwicklung darf sich aber nicht auf diese Kernkompetenzen begrenzen, sondern muss auch inhaltlich das Thema Informationssicherheit vollständig erfassen und bestenfalls selbst umsetzen.

DURCHFÜHRUNG

Die einzelnen Spiele sind durch eine Gesamtstory miteinander verknüpft. Jedes Serious Game enthält zwei bis drei Lernpfade. Am Ende erhalten die Teilnehmenden Feedback zu ihrem Spielerfolg sowie eine Zusammenfassung der Lessons Learned. Auch im Laufe des Spiels werden die Spielenden auf vorteilhafte oder nachteilige Entscheidungen und Verhaltensweisen aufmerksam gemacht. Zudem bietet ein Lexikonmodul Erläuterungen wichtiger Begriffe der Informationssicherheit.

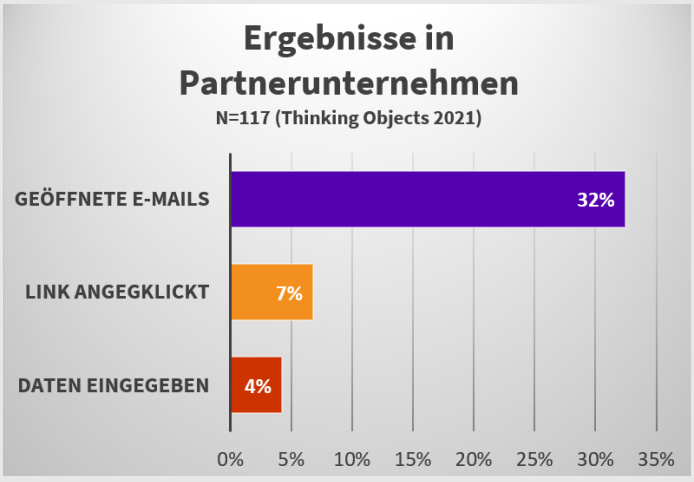
ERFOLG

Als kreatives Studio erarbeitete Gamebook für sich neue Sachinhalte, versetzte sich und Nutzende in Rollen von Opfern und Angreifenden und spielte seine Kernkompetenz, das Storytelling, voll aus. Das Unternehmen erweiterte nicht nur sein Portfolio durch ein sichtbares Gesellschaftsthema, sondern auch das eigene Informationssicherheitsbewusstsein. Als Ergebnis sind die sieben digitalen Serious Games ein gut in Trainingskonzepte integrierbares, durch betriebliche Vor- und Nachbereitung moderierbares und von Nutzenden eigenständig vertiefbares, hautnahes Erlebnis.

Vom vorsichtigen Angriff zum niederschwelligen Sicherheitskonzept

„…[unser] Portfolio nochmals im engen Austausch mit den Pilotunternehmen weiterzuentwickeln und neue Angriffssimulationen zu konzipieren und zu testen … ist ein großer Gewinn. … Ob eine Kampagne erfolgreich ist, zeigt sich am deutlichsten anhand der Feedbacks der Zielgruppe, nämlich den Mitarbeitenden.“

Martina Vogt, IT-Sicherheitsberaterin und Didaktikerin, Thinking Objects



MISSION:
Prüfung und Aufbau einer IT-Sicherheitsstrategie

Eigene Schwächen und der Umgang damit in der Praxis sind besonders wichtig bei der Analyse der Lage und Sicherheits- und Fehlerkultur in KMU sowie bei der Entwicklung von Handlungsempfehlungen, um Informationssicherheit zu stärken. Die Pilotunternehmen wurden zur Beurteilung der Anfälligkeit und Erhöhung der Resilienz über verschiedene Angriffsvektoren sensibilisiert. Besonders ethische Grundsätze, z. B. die Vermeidung von persönlichen Bloßstellungen, Störungen des Betriebsklimas oder Strafmaßnahmen, prägen eine professionelle Kampagnenbetreuung. Die Angriffe werden zudem eng in ein Awareness-Programm eingebettet und nicht inflationär verwendet, um rein positive Effekte zu erzielen und ein KMU bei der Optimierung von Prozessen, Meldewegen und Verantwortlichkeiten zu unterstützen.

PARTNERINNEN UND PARTNER
Pilotunternehmen
Mitarbeitende des Projekts (Angriffsziel)
Thinking Objects (Entwicklung)

KOOPERATION
Prüfung und Konzeption
Simulation

SCHWERPUNKT
Sensibilisierung in der Praxis
Anwendungsnahe Forschung
Niederschwellige Sicherheitskonzepte

Podiumsdiskussion von Pilotunternehmern und Thinking Objects beim Awareness Forum im April 2022. Vernetzung und Dialog bilden wichtige Bestandteile bei der Anpassung und Vermittlung von Sicherheitskonzepten für Geschäftsführungen und IT-Verantwortliche.

Übergabe des Awareness-Koffers durch die Projektleitung als Dank an Martina Vogt und Götz Weinmann von Thinking Objects.

HERAUSFORDERUNG

Vor-Ort-Angriffe simulieren nah am Social Engineering sehr individuell im KMU mit der Gefahr, wunde Punkte ungewollt zu verschlimmern. Jeder Schritt muss sowohl mit der Geschäftsführung als auch den Mitarbeitenden gefühlvoll vorbereitet und unter Achtung ethischer Grundsätze durchgeführt werden. Geschäftsabläufe dürfen nicht übermäßig gestört und Vermeidungshandlungen bezüglich der Compliance, Frustration oder Verlust von Selbstwirksamkeitserwartungen sollte entgegengewirkt werden.

DURCHFÜHRUNG

Aufklärung, Feingefühl und Förderung einer gesunden Fehlerkultur sind als wichtige Grundlagen durchgängig beachtet worden. Im direkten Austausch mit den Verantwortlichen stand ein rücksichtsvoller und maßvoller Umgang im Vordergrund. So wurden Maßnahmen nur nach Zustimmung durchgeführt, wenn alle Voraussetzungen, wie z. B. Diensthandys für Smishing oder keine Schocks bezüglich voriger Ransomware-Attacken, dafür erfüllt waren. Stets wurden Motivation, Zweck, Strategie, Ziele und Ergebnisse aufeinander abgestimmt und kommuniziert.

ERFOLG

Die vertraulichen Ergebnisse der Tests sind Grundlage einerseits der Erarbeitung individueller Sicherheitskonzepte und Ergreifung akuter Maßnahmen, anderseits KMU spezifischer, allgemeiner IT-Sicherheitsstrategien. Sieben Informationsblätter für Nutzende und niederschwellige Sicherheitskonzepte für Geschäftsführungen und IT-Verantwortliche wurden aus den „Vor-Ort-Angriffen“ des Projekts in KMU abgeleitet und online auf der Projektwebseite zur Verfügung gestellt.

Quid pro Quo: Forschungsbeitrag im Gegenzug für Aha-Erlebnisse

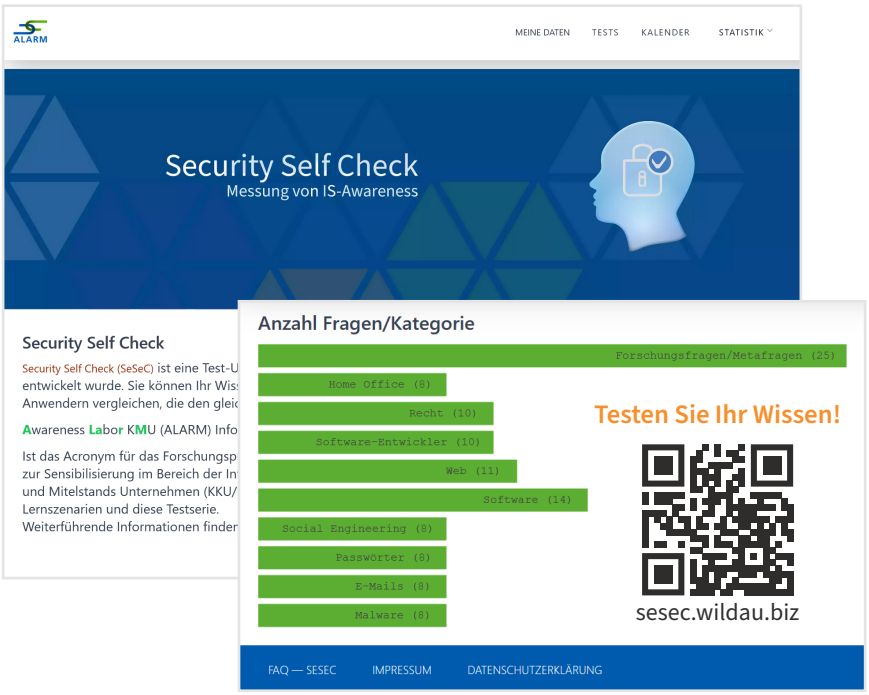
„Wir haben keine Zeit, Mitarbeitende über längere Zeit für umfassende Bildungsmaßnahmen freizustellen. … der personelle physische Tailgating-Versuch war sehr eindrucksvoll, … Wissenschaft sollte den Unternehmen etwas anbieten.“

Gerald Rynkowski, Geschäftsführer, Veinland

MISSION:

Einbindung der KMU in die Entwicklung praxisnaher Awareness-Messungen für Wirkungs- und Reifegradaussagen

Auch wenn der Projektname es anders suggeriert, Forschung an KMU erfolgt in keiner Laborumgebung, sondern am lebenden Objekt in freier Wildbahn. Sicherheit ist aber nicht so sehr ein Zustand als vielmehr ein komplexer Prozess. Die Kunst bei der Beobachtung besteht darin, scheues Wild, wie ein KMU, nicht zu verschrecken und weitgehend ungestört seinen Abläufen nachgehen zu lassen, obwohl Datenerhebung, Evaluationen und Befragungen einen erheblichen Aufwand für die Pilotunternehmen bedeuten. Kontinuierliche Fütterung mit verwertbaren Erlebnissen ermöglicht diese Symbiose.



PARTNERINNEN UND PARTNER

Pilotunternehmen
Studierende der TH Wildau

KOOPERATION

Testung, Messung und Evaluation

SCHWERPUNKT

Erprobung von Messkonzepten
Anwendungsnahe Forschung
Erhöhung des Selbsteinschätzungsvermögens

Übergabe des Awareness-Koffers durch die Projektleitung als Dank an Gerald Rynkowski.

Security Self Check (SeSeC) ist eine Test-Umgebung, um selbstständig das eigene Wissen in verschiedenen relevanten Informationssicherheitsthemen prüfen und mit anderen Anwenderinnen und Anwendern oder Gruppen vergleichen und auswerten zu können.

HERAUSFORDERUNG

Alle Maßnahmen müssen auf ihre Wirksamkeit hin überprüft werden, da sonst Prozesse nicht gesteuert und verbessert werden können. Geschäftsführungen sind stärker auf Ergebnisse fixiert, da Geschäftsabläufe kaum Raum für umfangreiche Evaluationen und Befragungen bieten. Ressourcen werden ungern vom Kerngeschäft abgezogen. Der Wert von unentgeltlichen Sensibilisierungsmaßnahmen wird nicht immer ausreichend wahrgenommen, teilweise darüber hinaus sogar eine Aufwandsentschädigung erwartet.

DURCHFÜHRUNG

Die Entwicklung der Serious Games wurde durch eine mit Test- und Kontrollgruppen sowie Pre- und Post-Tests gestützte Forschung begleitet, um die Wirksamkeit der entwickelten Maßnahmen zu evaluieren und neue Messkonzepte zu erproben. Matchingkonzepte durch Analysen, insbesondere partielle Ordnungen, versuchten einen Awareness-Indikator abzuleiten. Es wurde auf beständige und offene Kommunikation mit den Partnerinnen und Partnern und eine vielfältige Kombination der Maßnahmen geachtet, um das Interesse nicht abreißen zu lassen.

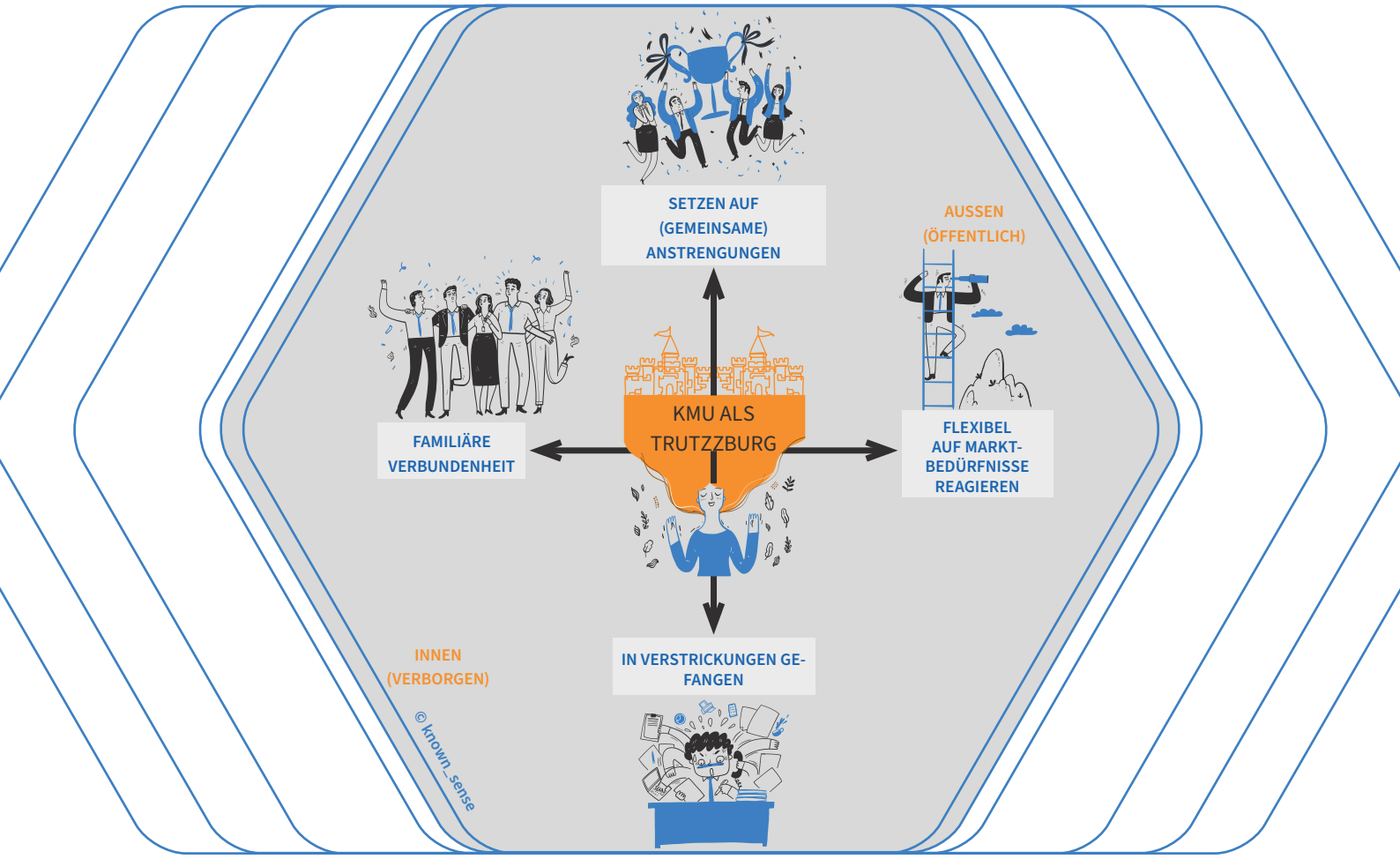
ERFOLG

Drei Pilotunternehmen konnten nachhaltig in einem komplexen Forschungsprojekt eingebunden, sensibilisiert und erforscht werden. Trotz Pandemie, volatiler Geopolitik und wirtschaftlicher Zwänge gelang es, genügend Erlebnisse, Erfahrungen und Verbündete zu erzeugen, die Sinn und Wert der Erhöhung des Awareness-Reifegrads unterstrichen. Die gesammelten Daten halfen dabei, die Serious Games auf eine fundierte Basis zu stellen. Der Security Self Check beispielsweise versetzt KMU in die Lage, selbst Wissen zu messen, zu vergleichen und zu verfolgen.

Anwendungsorientierte Forschung und neue Ideen für eine sichere Zukunft

„Security ist Kommunikation, Awareness ist Diskurs – wir alle können nur dann sicher agieren, wenn wir in einen permanenten Austausch mit anderen, aber auch mit uns selber kommen. Denn Selbstreflektion ist exakt die Fähigkeit, die wir brauchen, um andere, z. B. die Angreifer, beurteilen zu können,…“

Dietmar Pokoyski, Berater und Gründer von known_sense,
Autor von Studien und Entwickler der analogen Serious Games des Projekts



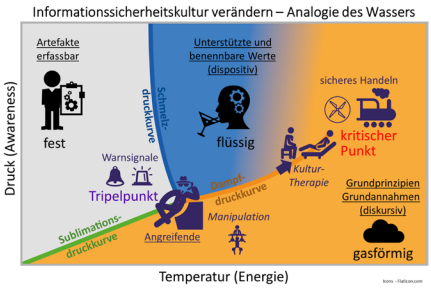
MISSION:

Ergründung und Vermittlung von Bewusstseinsebenen, Rollenverständnissen und Informationssicherheitskultur

Die qualitative, tiefenpsychologische Wirkungsforschung zu Informationssicherheit und Security Awareness bei KMU in Form von drei Studien zu Grundlagen, Konzept-/Produkttestung und einem Anwendungsleitfaden für die entwickelten Methoden wurde durch quantitative Umfragen und drei Berichte (Reports) begleitet. Die Berichte beschreiben die Ausgangslage, Informationssicherheitskultur und den Erfolg der verzahnten Methoden in KMU. Eine Vielzahl innovativer Konzepte ermöglicht es allen Teilhabenden, besser die Prozesse, Chancen und Risiken von Informationssicherheit in KMU zu erfassen und in ein Veränderungsmanagement zu integrieren.

Hier eine Auswahl:

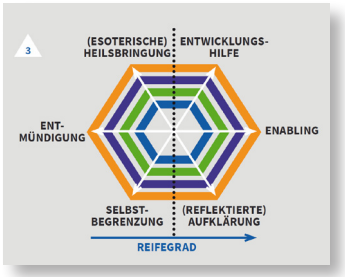
Report 1: Modularer Tätigkeitsprofilbogen



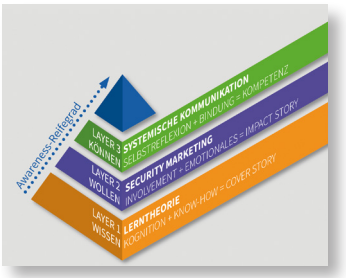
Report 2: Drei Aggregatzustände der Informationssicherheitskultur

Report 3: Erfolg der verzahnten Methoden

Studie 1: Typologien der Handelnden



Studie 2: Psychologische Spannungen von diskursiven Serious Games



Studie 3: Security-Awareness-Layer-Modell

PARTNERINNEN UND PARTNER

Pilotunternehmen
known_sense (Studien inkl. Leitfaden)

KOOPERATION

Umfragen, Interviews, Analyse

SCHWERPUNKT

Tiefenpsychologische Interviews
Entwicklung neuer Ansätze
Verbund von Theorie und Praxis

HERAUSFORDERUNG

Es besteht der Anspruch, eine Brücke zwischen wissenschaftlicher Forschung und praktischer Anwendbarkeit für KMU zu schlagen. Wie bei anderen Forschungsaufgaben standen die Datenerhebungen, Umfragen oder tiefenpsychologischen Interviews im Konflikt mit operativen Geschäftsaufgaben der Pilot-KMU. Genügend Teilnehmende mussten gesucht und bei geringer Repräsentativität Wege gefunden werden, aus den Daten den bestmöglichen Nutzen zu ziehen.

DURCHFÜHRUNG

Umfragen wurden quantitativen Forschungsstandards entsprechend konzipiert und adaptiert. In der zweiten Umfrage wurde ein Fragebogen an die Ansprechpersonen in den Pilot-KMU ergänzt, um die Auswahl der Stichprobe besser nachvollziehen zu können. Qualitative Interviews wurden in der zweiten Studie auf externe Teilnehmende erweitert, um die Pilotunternehmen zu entlasten. Dem Wunsch nach einem zusammenfassenden Anwendungsleitfaden wurde in der dritten Studie entsprochen und im zweiten Report ein Wegweiser zur praktischen Nutzung aller Projektergebnisse konzipiert.

ERFOLG

Unerwartet, aber dennoch wertvoll war, dass in KMU schwer differenzierbare Tätigkeitsprofile modular konzipiert wurden (siehe Abbildung zu Report 1), um Sensibilisierungsmaßnahmen auf die Bedürfnisse flexibel anzupassen. Zudem werden Verantwortliche ermuntert, Informationssicherheitskultur nicht ausschließlich durch Umfragen zu erfassen, sondern – im Einklang mit den Studienergebnissen – die familiären Verbindungen in KMU für ein empathisches Veränderungsmanagement zu nutzen. Nicht zuletzt die Studien bestätigten die Unentbehrlichkeit der Security Awareness.

Technische Hochschule Wildau
Technical University of Applied Sciences

Informieren Sie sich!

alarm.wildau.biz

Der vorliegende Report: **Gemeinsam zum Projekterfolg – Neue Wege für mehr Informationssicherheit in KMU** ist der letzte von insgesamt drei Berichten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ verfasst wurden. Aus sechs Arbeitspaketen werden sechs Erfolgsgeschichten gelungen verzahnter Methoden erzählt. Die Zitate der Success Stories wurden den Podiumsdiskussionen der Awareness Foren im April 2022 und Juni 2023 entnommen.

Projektlaufzeit

01.10.2020–31.03.2024

Das diesem Bericht zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) unter dem Förderkennzeichen 01MS19002A in der Initiative IT-Sicherheit in der Wirtschaft im Förderschwerpunkt „Mittelstand-Digital“ gefördert.

Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

September 2023

ISBN 978-3-949639-07-4

UNTERAUFTRAGNEHMER

gamebook · known_sense awareness you can touch. · sudile supported distance learning · Thinking Objects

ASSOZIIERTE PARTNER

IHK Cottbus · IHK Ostbrandenburg · IHK Potsdam · DIZ Digitales Innovations Zentrum