TAKE AWARE 2017

Die Security Awareness-Konferenz

TAKE AWARE 2017
Die Security Awareness-Konferenz

16. MÄRZ 2017 IN NEUSS

www.take-aware.com

Veranstalter

KIS Kompetenzzentrum Internationale Sicherheit
Rheinische Fachhochschule Köln
University of Applied Sciences

my breev

known_sense
awareness you can touch.

Partner

pallas

Medienpartner

eco

CORPORATE-SECURITY.TV

<kes>
Die Zeitschrift für Informations-Sicherheit

System Mensch - sensibilisieren Sie noch oder verändern Sie schon?

Mit der ersten Ausgabe der TAKE AWARE am 16. März 2017 stellen das Kompetenzzentrum Internationale Sicherheit (KIS) sowie die Awareness-Dienstleister mybreev und known_sense an der Rheinischen Fachhochschule Köln, Standort Neuss das neue Liveformat-Leitmedium für Mitarbeiter-Sensibilisierung, Sicherheits-Kommunikation und Veränderungsprozesse im Bereich Information Security, Datenschutz & Co. vor. Diese Praxiskonferenz wendet sich an alle Zielgruppen, die sich mit dem Themenkreis „Security Awareness" auseinander setzen.

Zur **TAKE AWARE** eingeladen sind insbesondere

- Security Manager, Awareness-Manager, CISO & Co.
- Datenschutzbeauftragte
- Business Continuity Manager
- Compliance-Beauftragte
- Kommunikationsexperten
- Change Manager
- Trainer
- HR-Mitarbeiter
- Studierende, Lehrende bzw. Forschende aus dem Umfeld der Informationssicherheit

Als Teilnehmer werden Sie durch die **TAKE AWARE** in die Lage versetzt, sowohl neueste Forschungsergebnisse und darauf basierende methodische Ansätze, als auch Praxisbeispiele für Medien, Tools und komplette Kampagnen direkt aus der Konferenz mit nach Hause bzw. an Ihren Arbeitsplatz zu nehmen, um sie innerhalb ihrer eigenen Organisation ad-hoc einsetzen zu können.

Awareness 2017 – Rundum-Beschallung oder Change-Prozess?

Mit dem Zugeständnis auch der letzten Zweifler an den hohen Stellenwert des menschlichen Faktors zugunsten sichererer Systeme, Informationen und Organisationen hat Security Awareness 2016 ihre „Unschuld verloren". Können wir unmittelbar nach beinahe alltäglichen und spektakulären Hacks, weiteren Cyber Crime-Vorfällen und Security- bzw. Privacy Incidents in punkto Sensibilisierung so weitermachen wie bisher? Hier ein bisschen Wissensvermittlung mit einer Prise WBTs, dort das Schwarze Brett oder dünne Erklärfilmchen? Das alles mit „Schrotflintenansatz", d.h. ohne Zielgruppen-Differenzierung? Oder braucht Awareness nicht vielmehr ein modulares Methodenportfolio, das die Black Box „Mensch" quasi psychologisch „hackt" und entschlüsselt und ein strategisches Vorgehen für Organisationen aller Größen, Branchen und Kulturen zulassen würde?

Keynote: Symptom oder Ursache?

„Klassische Security Awareness Ansätze kurieren lediglich ‚Symptome' ohne die Ursachen menschlichen

TAKE AWARE – das nehmen Sie mit:

- Bewährte und innovative Awareness-Methoden
- Praxisbeispiele und Konzepte für Kampagnen und Tools aus zahlreichen Behörden, Unternehmen sowie von Awareness-Dienstleistern
- Neueste Forschungsergebnisse aus internationalen Hochschulen und von erfahrenen Tiefenpsychologen
- Konkrete Sinnes-Erfahrungen aus Table Talks , Mitmach- und Gamification-Settings
- Austausch auf Augenhöhe mit Kolleginnen und Kollegen aus Deutschland, Schweiz und UK
- Viele Ideen und Motivation für eigene Konzepte, Medien und Maßnahmen

(Fehl-)Verhaltens im System ‚Unternehmen' zu hinterfragen", sagt Michael Helisch, u. a. Gründer von HECOM Security Awareness Consulting. Hier setzt seine Keynote „Sensibilisieren Sie noch oder verändern Sie schon?" an, mit der er die **TAKE AWARE** eröffnen wird und Sie davon überzeugen möchte, dass ein Perspektivwechsel in Richtung Change Management bzw. Veränderungsprozesse angebracht ist.

Methoden, Best Practice und Table Talks in kleiner Runde

Neben solchen und verwandten Vorträgen zur methodischen Herangehensweise bzw. zu verschiedenen Forschungsprojekten werden Ihnen aber auch Kampagnen-Praxisbeispiele direkt aus den Organisationen begegnen. Am Nachmittag werden Sie zum Teil der „Security-Awareness-Expertenrunde", indem Sie sich im Rahmen von überschaubaren Table Talks mit maximal 12 Teilnehmern aktiv auf verschiedene Impulsvorträge beziehen und innerhalb dieser kleineren, gegenüber klassischen Keynotes eher intimeren Gesprächs- und Austauschrunden mit Ihrer Meinung oder Ihren detaillierten Fragen einbringen können.

Live Hacking & Gamification in Team-Settings

Darüber hinaus haben Sie auch die Möglichkeit, in die Rolle Ihrer Zielgruppe zu schlüpfen und weltweit erprobte Maßnahmen auszuprobieren, z. B. beim Lunch & Learn Live Hacking der innogy SE, „Cyber-Bedrohungen am Arbeitsplatz und zu Hause live erleben", oder indem Sie an einem „SECURITY PARCOURS" teilnehmen. Bei diesem bereits 2013 vom ISF als „innovativste Awareness-Maßnahme" ausgezeichnetem Lernstationsformat von T-Systems, das den diskursiven Lernaspekt „Talking Security" (Reden über Sicherheit) in den Fokus rückt, bewegen Sie sich als Mitglied eines Teams wie bei einem Circle-Training durch einen Parcours und durchlaufen dabei verschiedene Awareness-Stationen mit „Minigames".

Meet & Greet: „Wölfe & Geißen" lockt wie einst Rotkäppchen mit u. a. Kuchen und Wein

Falls Sie bereits am Vorabend der Konferenz anreisen, sind Sie herzlich zum Meet & Greet unter dem Titel „Wölfe & Geißen" ab 18:30 Uhr, ebenfalls in Neuss, eingeladen. Dieser Vorabend-Event ist eine Wiederbelebung des 2008 in Köln gegründeten, so genannten Rheinischen Security-Stammtisches. In dieser aktuellen Ausgabe wird Dr. Christoph Schog, Security Manager bei T-Systems International, gemeinsam mit seinen Awareness-Kollegen und -Kolleginnen die Arbeit des „Dax-30 -Roundtable Security Awareness" (u. a. mit EnBW, Bosch, Lufthansa, Munich Re, innogy/RWE, SAP) vorstellen.

Awareness-Benefits auf einen Blick:

- Schärfung einer widerspruchsfreien Sicht auf **sämtliche** Sicherheitsthemen
- Vermittlung von Security Policies und Erklären der dort aufgeführten Regeln
- Vermittlung der Ziele von Informationssicherheit und der positiven Auswirkung auf das Unternehmen bei Erreichen dieser Ziele und – umgekehrt – der negativen Folgen bei Nichteinhaltung der Regeln
- Vermittlung der Wirksamkeit des eigenen Verhaltens (Mitarbeiter als Teil einer „Human Firewall")
- Vermittlung der persönlichen Vorteile, die durch sicherheitskonformes Handeln erzeugt werden
- Vermittlung von Kompetenzen bei allen Beschäftigten hinsichtlich der praktischen Anwendung von Security-Regeln und von unterstützenden Tools innerhalb des Arbeitsalltags
- Positionierung von Sicherheit und Security-Teams durch die nachhaltige Werbung für Security-Themen, -Aufgaben, -Tools und -Protagonisten zur Steigerung von Akzeptanz auf allen Ebenen
- Unterstützung von Führungskräften, damit diese ihren Aufgaben als Security-Vorbild und -Multiplikator gerecht werden können
- Kundenbindung sowie grundsätzlich positive Positionierung des Unternehmens-Image gegenüber Partnern und der Öffentlichkeit

TAKE AWARE IM ÜBERBLICK

Termine und Ort

- **Do., 16. März 2017, 9:00 bis 17:00 Uhr**

Rheinische Fachhochschule Köln, Standort Neuss
Markt 11-15, 41460 Neuss, Tel.: +49 02131/73986-0

- **Mi., 15. März 2017, ab 18:30 Uhr: „Wölfe & Geißen“**

als Meet & Greet (Konferenz-Vorabend-Event),
Neuss (Location wird noch bekannt gegeben)

Preise, Anmeldung, Sponsoring, Kontakt

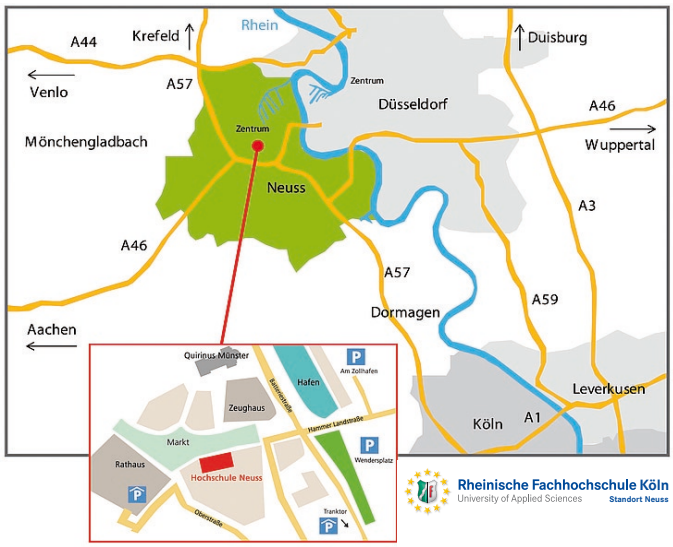
- Normaltarif: 290,00 Euro (netto)
- Frühbucher-Rate: 195,00 Euro (bis 15.02.2017, netto)
- Studententarif: 60,00 Euro (netto)

Anmeldung unter www.take-aware.com
Die Anmeldung ist verbindlich. Bei Stornierung werden 65 Prozent der Gebühr fällig. Meet & Greet ist inklusive! Mitglieder von eco e.V. erhalten 20% Rabatt.
Sponsoring: Drei Angebote unter www.take-aware.com
Bei Fragen: +49 2203/1831618 oder +49 2162/1065549

Übernachtungen

Reisen Sie am Vortag an und/oder erst am Tag nach dem Kongress ab und benötigen Sie ein Hotel? Wenden Sie sich an das Dorint Kongresshotel Düsseldorf/ Neuss (ab 115,00 €, 700 m zur RFH, ****), Stichwort „TAKE AWARE“

Anfahrt RFH Köln, Standort Neuss



Referenten und Moderatoren:

- Holger Berens (Rheinische Fachhochschule Köln, Leiter Kompetenzzentrum Internationale Sicherheit – KIS)
- Marcus Beyer (Hewlett Packard Enterprise, Schweiz)
- Thomas Bleuel (E.ON Business Services)
- Sebastian Feik (Legitimis)
- Dr. Käthe Friedrich (BAköV – Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern)
- Ulrich Gärtner (Pallas)
- Michael Helisch (HECOM Security Awareness Consulting)
- Udo Hempe (Rheinische Fachhochschule Köln, Standortleiter Neuss)
- Sebastian Klipper (CycleSEC)
- Sascha Maier (IWC Schaffhausen, Schweiz)
- Thomas Müller (Aduno Gruppe, Schweiz)
- Dietmar Pokoyski (known_sense)
- Dipl. Psychologin Ivona Matas (known_sense)
- Vitali Regehr & Thomas Krauhausen (innogy SE)
- Uwe Röniger (mybreev)
- Prof. Dr. Angela Sasse (Director UK Research Institute for Science of Cyber Security RISCS, UK)
- Klaus Schimmer (SAP AG)
- Dr. Christoph Schog (T-Systems International)
- Prof. Dr. Margit Scholl (TH Wildau)

Praxisbeispiele aus den deutschen Behörden, von der Aduno Gruppe sowie von E.ON, HPE, innogy/RWE, IWC Schaffhausen, known_sense, Legitimis, mybreev, Pallas, RISCS, SAP, TH Wildau, T-Systems/Deutsche Telekom u.v.m.

Abb. known_sense aus dem Security Awareness-Kalender 2017 (Illustrationen von freepik.com, known_sense, Neubauwelt)