Wenn der Ernstfall eintritt:
Die Rolle der Cybersecurity-Awareness bei Cyberangriffen.

PROJEKTBEISPIEL

KISK: Kompetenzbasierte Entwicklung von ITS-Trainingsangeboten in Krankenhäusern

Dr. Kristin Masuch

Expertin im Bereich Crisis Management, Disaster Recovery Strategies und „Security, Training, Awareness, and Education“ (SETA)

Studierte Wirtschaftsinformatikerin/ promoviert im Bereich Cybersecurity (Security Crisis Recovery)	Co-Founderin der CySec Cybersecurity with IQ
Dozentin im Bereich „Enterprise Cybersecurity“	Mehrjährige Erfahrung im (Informationssicherheits-) Projektmanagement
Zertifizierte ISO 27001 Beraterin & Projektmanagerin	Sprecherin zu aktuellen Cybersecurity Thematiken (u.a. TakeAWARE)

Projektleitung:

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

UNIVERSITÄTSMEDIZIN GÖTTINGEN : UMG

UNIVERSITÄT HOHENHEIM

Verstetigungspartner:

CySec
Institut für Cybersicherheit und Compliance

Assoziierte Partner:

UNIVERSITÄTS-KLINIKUM MAGDEBURG A.Ö.R.

UKR Universitätsklinikum Regensburg

Universitätsklinikum Erlangen

Ökumenisches Hainich Klinikum gGmbH

medbo®

EVANGELISCHES KLINIKUM Bethel

UNIVERSITÄTS KLINIKUM ulm

UNIVERSITÄTSKLINIKUM AUGSBURG

KLINIKUM OBERBERG
Rundum gut versorgt.

Carl-Thiem-Klinikum Cottbus
AKADEMISCHES LEHRKRANKENHAUS DER CHARITÉ

Unfallkrankenhaus Berlin

MHH Der Gesundheits-Campus
Medizinische Hochschule Hannover

PROBLEMSTELLUNG

Der Arbeitsalltag in Unternehmen führt zu Herausforderungen bei der Umsetzung von ITS-Maßnahmen

Maßnahmen
…zur Steigerung der mitarbeiterbezogenen IT-Sicherheit

Anwendung
… von Prozeduren und Werkzeugen zur Gewährleistung der IT-Sicherheit

Problem ITS-Interventionen weisen eine geringe Effektivität auf und führen zu geringer Anwendung von ITS-Prozeduren im Krankenhausalltag

Ursache **Fehlende Kompetenzorientierung**
a) Unklarheit bzgl. der tatsächlichen Kompetenzbedarfe
b) Trainings orientieren sich nicht am tatsächlichen Qualifizierungsbedarf
c) Keine anforderungsorientierte Evaluation der Interventionseffektivität
d) Geringe Motivation für das Thema bei Schulungen und der Anwendung

Lösung
a) Kompetenzmodellierung zeigt Kompetenzbedarf
b) Kompetenzaufbau durch zielgerichtete Interventionen
c) Kompetenzmessung ermöglicht nachhaltige Verhaltensänderung und wissenschaftlich evaluierte ITS-Awareness-Toolkits
d) Nachhaltiger Trainingserfolg und Verhaltensänderung durch ITS-Nudges

Ganzheitliche IT-Sicherheitsstrategie je Domaine

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 erforderlich sind, um konzeptionelles Wissen in bestimmten Handlungssituationen anzuwenden.
Wann?	Interpretierende Kompetenz	Kognitives Erkennen der Anforderungssituation und Wissen über angemessene Interpretation und Validierung der Situation.
Warum?	MotivationaleKompetenz	Grundlegende motivationale und affektive Merkmale in bestimmten Handlungssituationen.

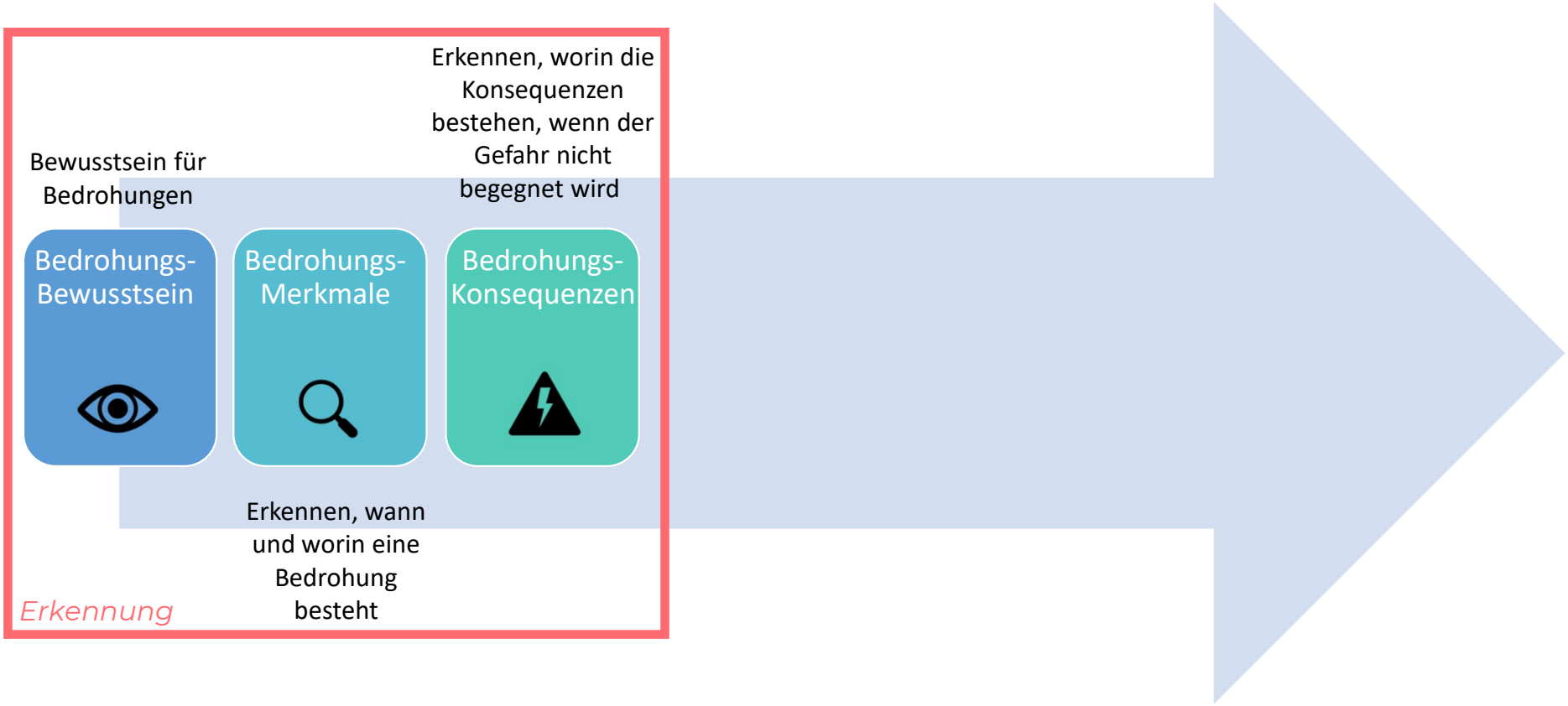
Jemand ist gut qualifiziert sich informationssicher zu verhalten:

- Wissen über ITS-Bedrohungen & ITS- Maßnahmen
- Anwendung von ITS-Maßnahmen
- Erkennen von ITS-Bedrohungen
- Auswahl der besten Gegenmaßnahmen
- Bewertung der Gegenmaßnahmen
- Motivierende Faktoren

Security Baukasten

* Beruhen auf Kompetenzmodell

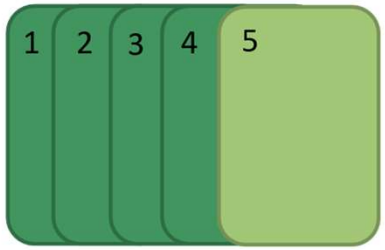
Notwendige Stufen für die Erkennung, Meldung und Eindämmung eines Angriffs



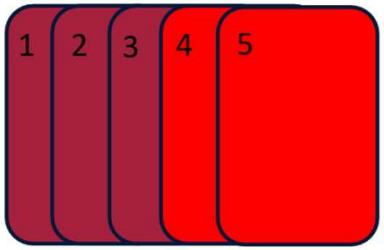
EXKURS:

Zielgruppen für Security Awareness-Inhalte im Klinikum

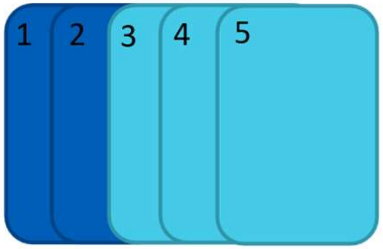
AP1: Verwaltung/Sachbearbeitung
(z. B. Case Manager, Abrechnung)



AP2: Medizinisches Fachpersonal
(z. B. Kinderkrankenpflege, MTR)



AP3: Arzt/Ärztin
(z. B. Kinderarzt, Radiologe)



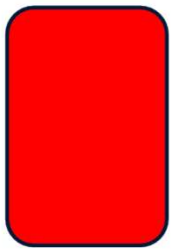
Viel Patientenkontakt / Behandelnd

Wenig Patientenkontakt / Verwaltend

Behandelnd

Verwaltend

Behandelnd

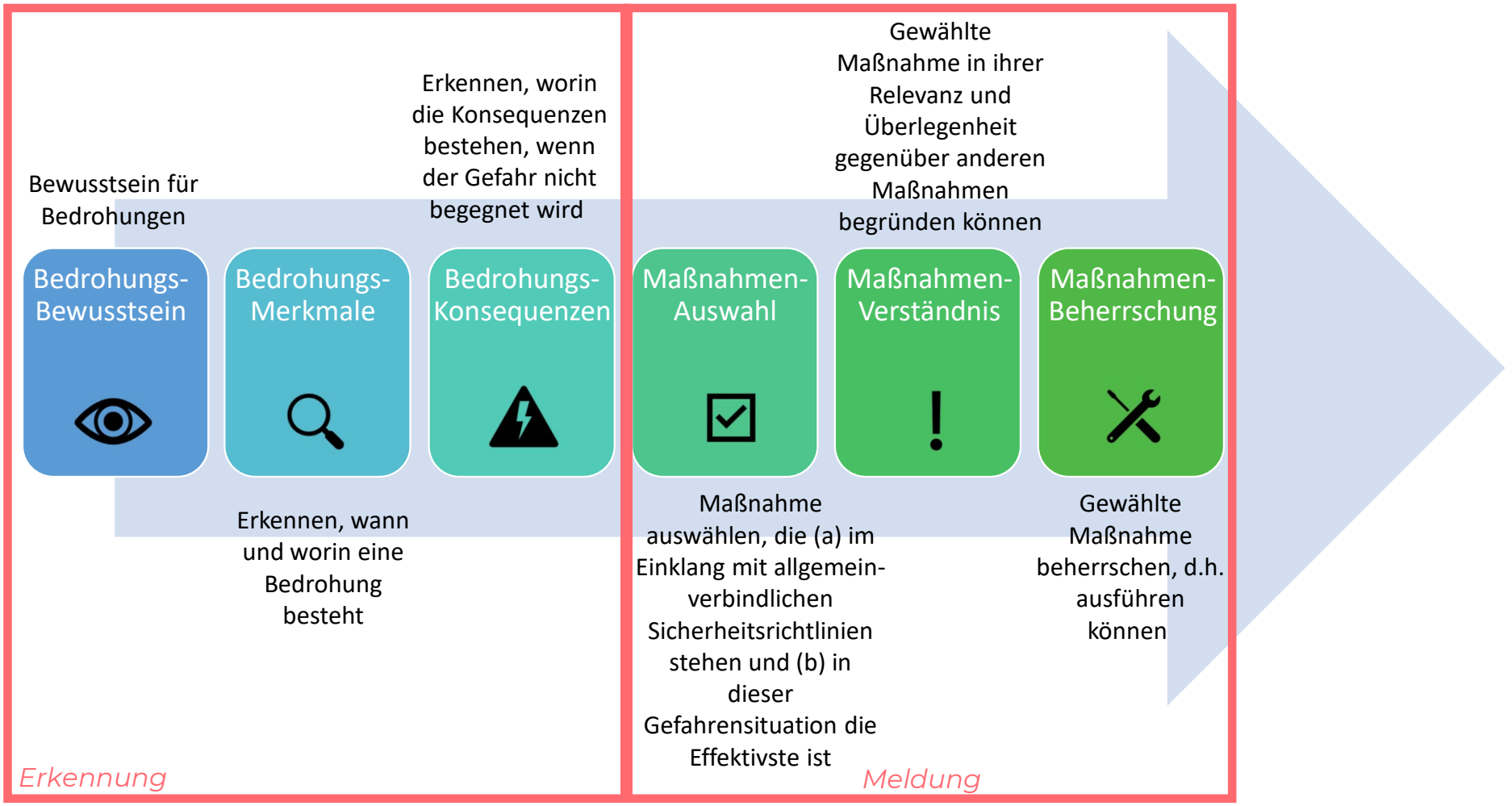


Verwaltend

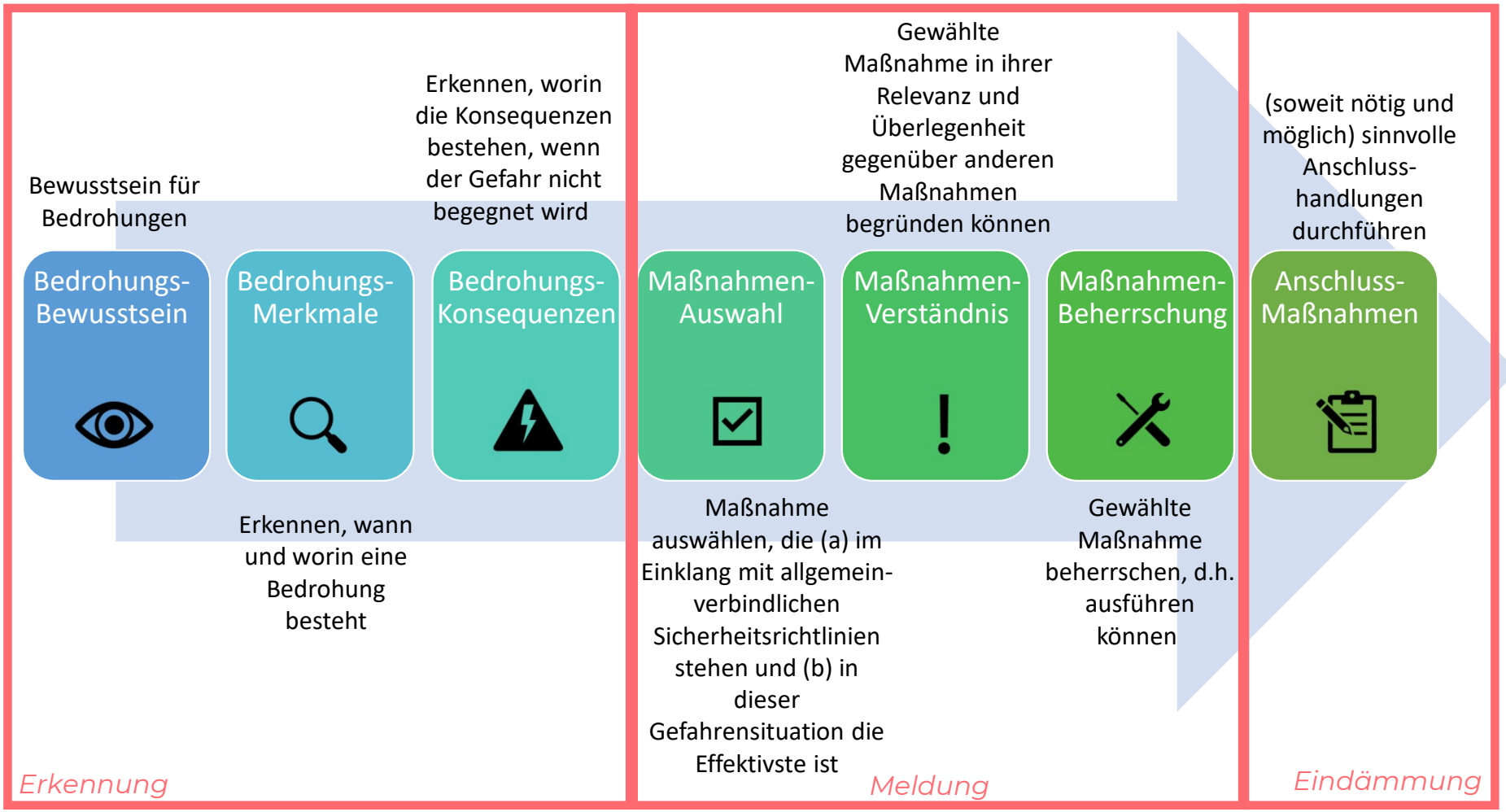
Behandelnd

Verwaltend

Notwendige Stufen für die Erkennung, Meldung und Eindämmung eines Angriffs



Notwendige Stufen für die Erkennung, Meldung und Eindämmung eines Angriffs



BEISPIEL

Security Baukasten – Ganzheitliche IT-Sicherheitsstrategie je Domaine

1. Anschlusshandlungen

Bspw. aufmerksame Mitarbeitende, die Phishing-Mails erkennen, schnell intern meldet **und** ihr Kollegen und Kolleginnen warnen.

2. Sicherheitskultur

Bspw. Mitarbeitende, die herumliegende Patient*innenakten sofort verstauen und Kollegen und Kolleginnen, die dies nicht tun über die Risiken von unachtsamem Umgang mit sensiblen Daten aufklären.

3. Interne Prozesse

Bspw. aufmerksame Expert*innen, die sich über einen gewissen Zeitraum herauskristallisieren Phishing-Mails zuverlässig zu erkennen und schnell intern zu melden. Wenn diese eine solche E-Mail melden, ist sofort klar, dass es sich um eine echte Bedrohung handelt und die Meldung wird vorrangig bearbeitet.

Krisenstab

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Kristin Masuch
CySec - Cybersecurity with IQ GmbH
Nikolausberger Weg 32, 37073 Göttingen

Telefon: (+49) 0152 26457 211
E-Mail: kristin.masuch@cysec-institut.de

September Veranstaltungen:

10.09.2025: IT-Sicherheitstage (NIS2 & Security Awareness - Paderborn)

11.09.2025: Big Bang KI Health Festival (EU AI Act: Cyber- und KI-Kompetenz im Gesundheitswesen - Berlin)