

Wirkungsvolle Umsetzung von IT-Compliance & - Awareness



Dr. Kristin Masuch

Co-Gründerin und
Geschäftsführerin

Studierte
Wirtschaftsinformatikerin

Promoviert im Bereich
Informationssicherheit, Fokus
Security Crisis Recovery

Mehrjährige Erfahrung im
(Informationssicherheits-)
Projektmanagement

Zertifizierte Projektmanagerin
& ISO 27001 Beraterin

Prof. Dr. Simon Thanh- Nam Trang

Co-Gründer

Studierter und promovierter
Wirtschaftsinformatiker

Professor für nachhaltige
Informationssicherheit an der
Universität Paderborn

Mehrjährige Erfahrung im
Informationssicherheits-
management im KRITIS-Sektor

Zertifizierter
Projektmanager & ISO 27001,
CISSP, ITIL, TOGAF



Projekte in 2023/24



innovativ.
flexibel.
zuverlässig.

Stadtwerke
Bielefeld



Kreis
Paderborn

...nah bei den Menschen!

ITS. Kompetent



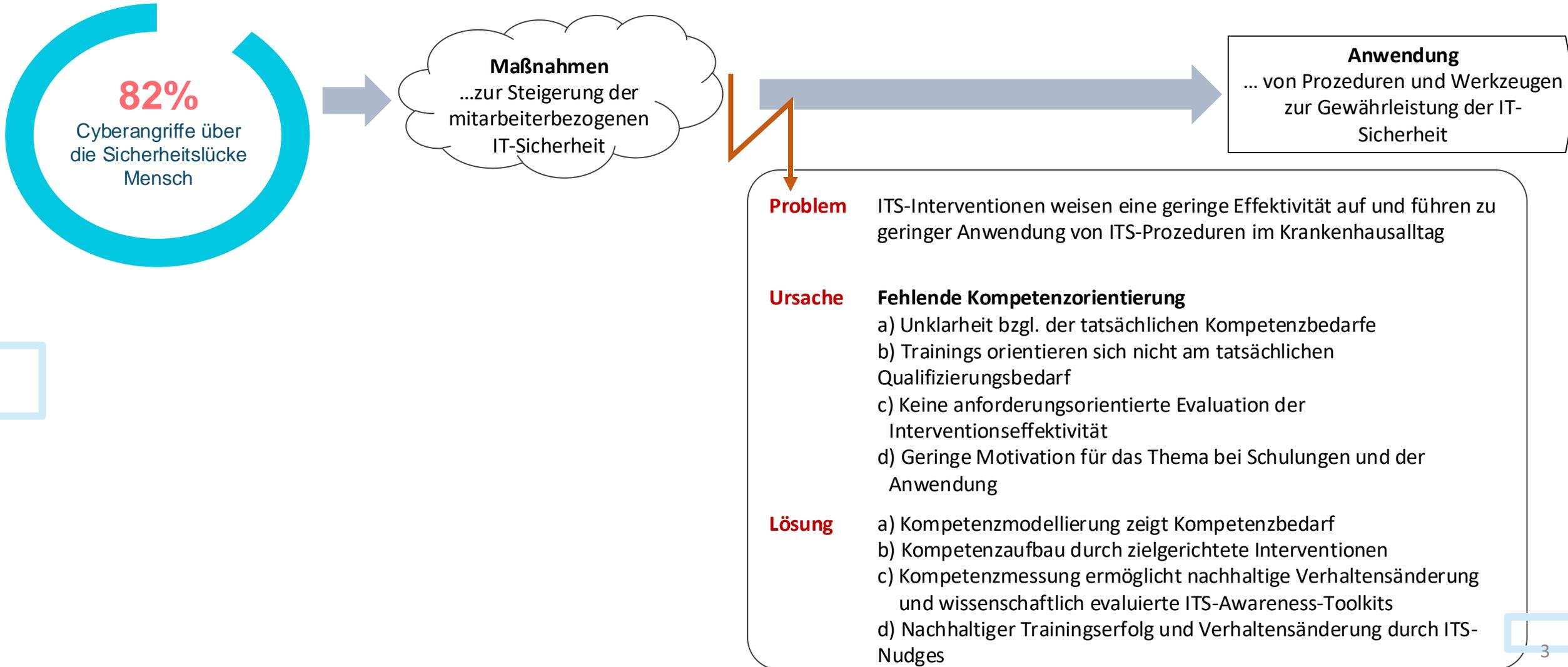
KISK

Kompetenzorientierte und stellenspezifische
IT-Sicherheit für Mitarbeiter:innen in Krankenhäusern



PROBLEMSTELLUNG

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



TEIL 1 + 2

ITS.kompetent

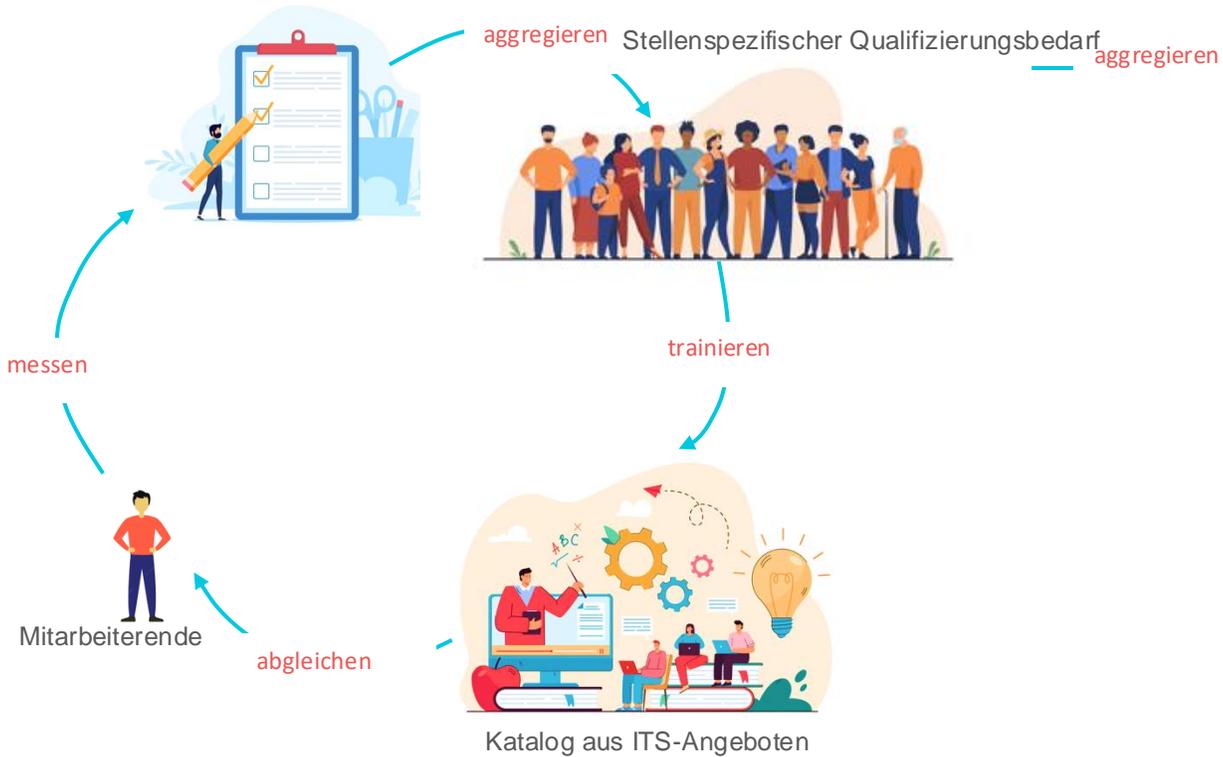
ITS.KOMPETENT: KMU-Mitarbeiter und -
Entscheider können sich zielgerichtet und
effizient in IT-Sicherheit durch die
Vermittlung passgenauer Trainingsinhalte
professioneller Anbieter weiterbilden.

METHODEN: Kompetenzmessung, Matching-
Verfahren, Data Collection, Field Studies,
Web Platform Architecture Development

ZEITRAUM TEIL 1: 2021 – 2024

ZEITRAUM TEIL 2: 2024 – 2027

ITS-Kompetenzmessinstrument gemäß
Anforderungsprofil



50%

KOMPETENZDIMENSION

- Konzeptionelle Kompetenz
- Prozedurale Kompetenz
- Interpretierende Kompetenz
- Motivationale Kompetenz

EMPFEHLUNG
TRAINING:

- Bedrohung A & B mit Fkus 1. Kompetenzdimension
- Bedrohung A,B & C mit Fkus 4. Kompetenzdimension

TEIL 1 (ABGESCHLOSSEN UND KOSTENLOS FÜR KMUs) ITS.kompetent



1 ITS-Anforderungsprofil bestimmen

IT-Admin

Herr Laimer ist IT-Admin. Er ist verantwortlich für die Administration, Überwachung und Wartung der IT-Infrastruktur des Unternehmens. Mit seinen umfassenden IT-Kenntnissen und Erfahrungen stellt er sicher, dass alle IT-Systeme und Netzwerke reibungslos funktionieren und den Sicherheitsrichtlinien entsprechen.

Auswählen

TÄTIGKEITEN

- Administration, Überwachung und Wartung der IT-Infrastruktur
- Sicherstellung des reibungslosen Betriebs von IT-Systemen und Netzwerken
- Umsetzung von Sicherheitsrichtlinien und Schutz vor Cyberbedrohungen
- Unterstützung von Mitarbeitern bei IT-Fragen und Problemen

2 ITS-Kompetenzen messen

ITS.kompetent

Scenario 1: A text message from +49 1738967453: "Nachrichte und Anrede sind richtig. Ende verschweigt. Niemand darf auf das Chat kommen sie lesen oder antworten." Reply: "Halo, ich habe meinen Koffer auf der Dienstreise verloren. Auch mein Handy ist dabei. Können Sie mir helfen?"

Scenario 2: A text message from +49 1738967453: "Nachrichten und Anrede sind richtig. Ende verschweigt. Niemand darf auf das Chat kommen sie lesen oder antworten." Reply: "Halo Herr Schmidt, ich habe meinen Koffer auf der Dienstreise verloren. Auch mein Handy ist dabei. Können Sie mir helfen?"

Scenario 3: A text message from +49 1738967453: "Halo Herr Schmidt, können Sie mir die Telefonnummern und Email Adressen von den Kunden schicken, die ich besuchen will. Vielen Dank." Reply: "Mig Sebastian Müller"

Buttons: Tests, Erste Testfrage anzeigen

3 ITS-Statistiken erhalten

Sozial Engineering / Social Media Systeme	Social Engineering / Instantmessenger
Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.	Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.
50%	86%
KOMPETENZDIMENSION	KOMPETENZDIMENSION
<ul style="list-style-type: none"> ⚠ Threat Awareness ✓ Threat Identification ✓ Threat Impact Assessment ✗ Tactic Choice ✓ Tactic Justification ✗ Tactic Mastery ✗ Tactic Check & Follow-Up 	<ul style="list-style-type: none"> ✓ Threat Awareness ✗ Threat Identification ✓ Threat Impact Assessment ✓ Tactic Choice ✓ Tactic Justification ✓ Tactic Mastery ✓ Tactic Check & Follow-Up
EMPFEHLUNG	EMPFEHLUNG
Basierend auf den Ergebnissen aus Ihrem ITS-Kompetenztest könnte ein ITS-Training im Bereich Social Engineering Ihre ITS-Kompetenzen verbessern.	Basierend auf den Ergebnissen aus Ihrem ITS-Kompetenztest benötigen Sie kein Training im Bereich Social Engineering

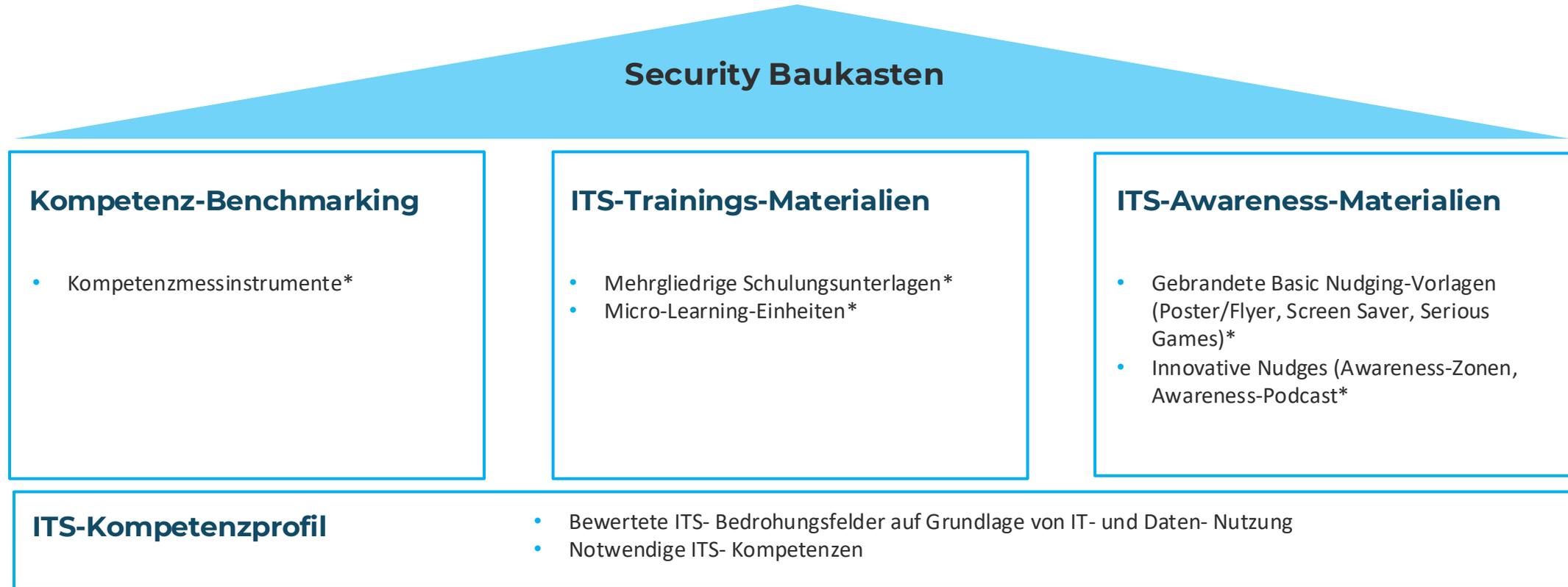
4 ITS-Trainingsempfehlungen erhalten

SETA PROGRAMM	ANBIETER	METHODE	INHALT	SCHWIERIGKEITSGRAD	KOSTEN	REGISTRIERUNG
Awareness-Kampagne Cybersecurity	Bayern Innovativ	Webinar/Video	Social Engineering Phishing Errechnen von Mäware Durchführung von Brute-Force-Angriffen deversuchen/Passworterrangriff	Sehr einfach (Grundlagen)	Kostenlos	Nein
Bereitschaft-Tests	Bundeskarte ID Sicherheit in der Informationsbranche	Webinar/Video	Phishing Errechnen von Mäware Kompromittierung von Informationssystemen Ausnutzen schwach konfigurierter Systeme Shpping (Service Beting) Durchführung von Brute-Force-Angriffen deversuchen/Passworterrangriff Denial-of-Service-Angriffe (DDoS) Ausnutzung von Multi-Tenancy in einer Cloud-Umgebung Ausnutzen bekannter Schwachstellen in mobilen Systemen (z. B. Laptops, PDAs, Smartphones)	Sehr einfach (Grundlagen)	Kostenlos	Nein



HOW-TO: STATE OF THE ART SECURITY AWARENESS

Security Baukasten



BEISPIEL

Security Baukasten – Ganzheitliche IT-Sicherheitsstrategie je Domaine

Anforderungsprofile

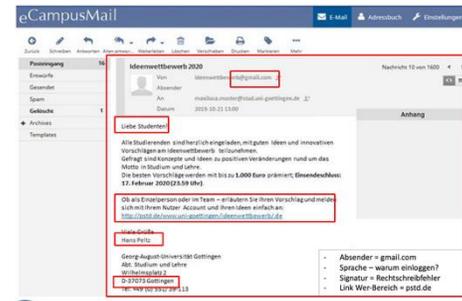


Messinstrumente

Sie sind derzeit für einen Patienten zuständig, auf dessen Blutprobe Sie schon den ganzen Tag warten, um die medikamentöse Einstellung vorzunehmen und dem Stationsarzt, Herrn Köhler, mitzuteilen.

Welche der folgenden möglichen Situationen ist die größte Bedrohung für die Informationssicherheit der Universitätsklinik Grüning?

- Sortieren Sie nach folgendem Schema:
- [1] Die Situation ist am bedrohlichsten.
 - [2] Die Situation ist weniger bedrohlich.
 - [3] Die Situation ist am wenigsten bedrohlich.



Trainings-Material



Awareness-Material

Würden Sie vertrauliche Informationen per Postkarte versenden?



Eine E-Mail ist wie eine Postkarte!





BAUSTEIN 1: KOMPETENZ-ANFORDERUNGEN

Erhöhung der Trainings-Effektivität und Reduktion der Trainingszeit durch Kompetenz-Anforderungsprofile

Schritt 1: Identifikation der Zielgruppe in der Domäne

Schritt 2: Klassifikation der Objekte in der Domäne
Bestandteile einer Sicherheitsbedrohung

Ergebnis: Kompetenz-Anforderungen
Rolle: Ärztin / Arzt

Schritt 3: Identifikation der Objekte in der Domäne
Cyber Security Domänen-Modell im Gesundheitswesen

Wichtige Assets	Bedrohungen
Informations-Assets	Identifizieren, Diagnose, usw.
Software-Assets	Web, Patientenportal, usw.
IT-Assets	LaTeX, Smartwatch, Smarte PC, usw.
Zentrale Bedrohungsvektoren	Cloudservices, usw.

Leitfrage: Welche Kompetenzen benötigen verschiedene MitarbeiterInnen?

Ergebnis

- Kompetenz-Anforderungsprofile: bspw. Geschäftsführung, Außendienst, IT-Admin, Ärzt*in, Medizinische Fachkraft, Verwaltungsfachkraft alles je mit und ohne Patient*innenkontakt
- Assets: u.a. Informationen, Software, Physische Assets
- Gewichtete Bedrohungen
- Kompetenz-Linien
- Kompetenzmessinstrumente

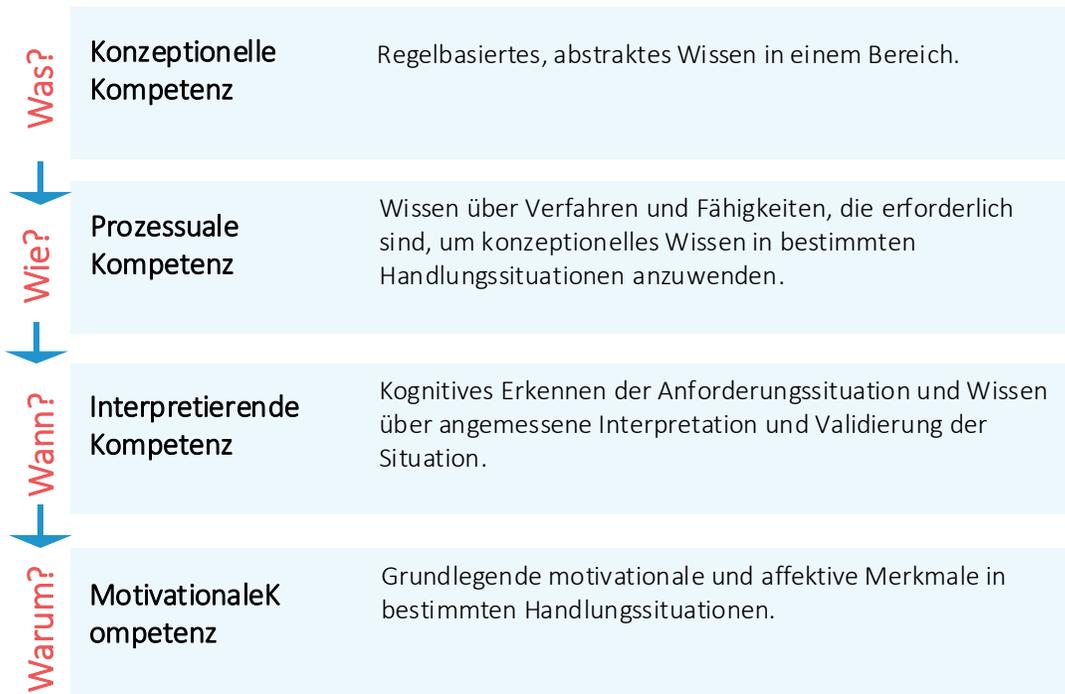


Ranking der Bedrohungsvektoren Profil: ärztliches Fachpersonal

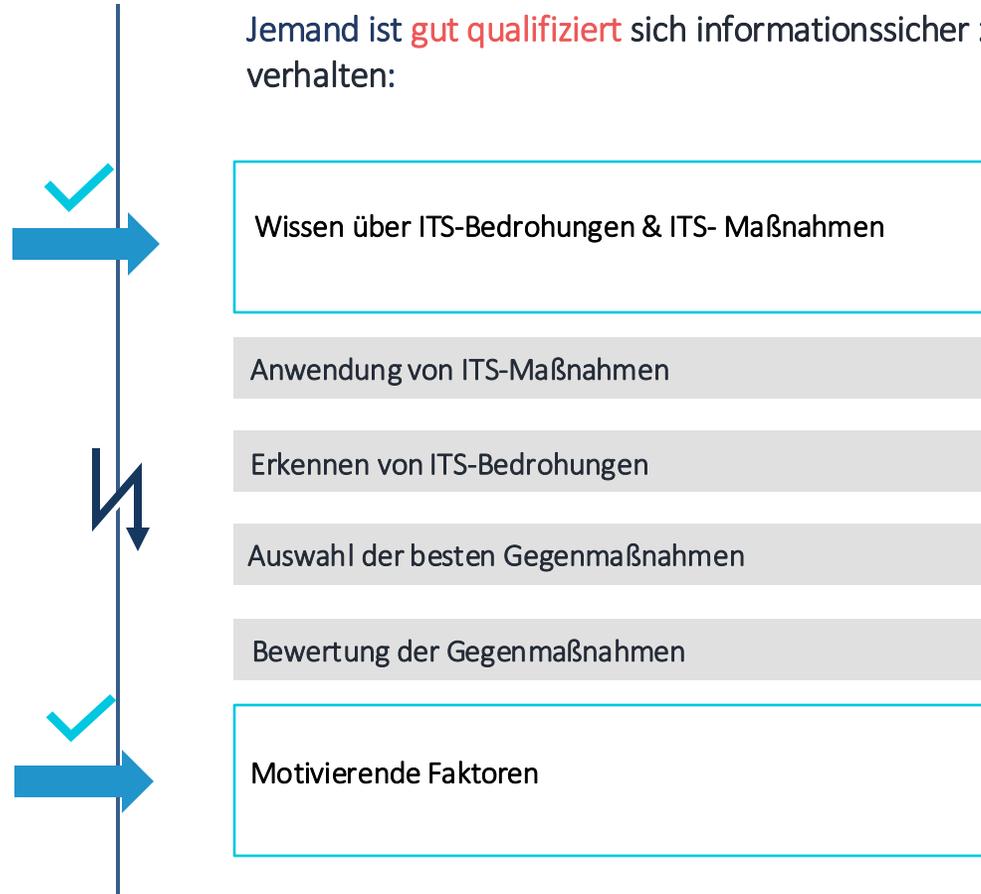
Nr.	Relevante Bedrohungsvektoren (d.h. Bedrohungsereignis & Kritisches Asset)	
1.1	Falscher Umgang mit kritischen und/oder sensiblen Informationen durch autorisierte Benutzer / KIS oder Mitarbeitende	Ein autorisierter, privilegierter Benutzer gibt versehentlich kritische/sensible Informationen bei Nutzung des KIS preis.
1.2	Angreifer erstellt Duplikate legitimer Internetseiten und leitet die Mitarbeitende auf gefälschte Internetseiten, um Informationen zu sammeln (z.B. Duplizierung einer Internetseite eines Lieferanten) / Internet-Browser	Typische Angriffe erfolgen per E-Mail, Instant Messaging oder auf vergleichbare Weise; dabei werden die Benutzer in der Regel auf scheinbar legitime Websites geleitet, während die eingegebenen Informationen in Wirklichkeit gestohlen werden.
1.3	Einschleusen falscher, aber glaubwürdiger Daten/Informationen in organisatorische Informationssysteme (z.B. von Insidem) / KIS	Ein autorisierter Benutzer verunreinigt irrtümlich ein Gerät, ein Informationssystem oder ein Netzwerk, indem er Informationen mit einer Klassifizierung/Sensibilität darauf ablegt oder an sie sendet, zu deren Handhabung er nicht autorisiert wurde.
1.4	Einschleusen bekannter Malware an interne Informationssysteme (z.B. Viren über unsichere Internetseiten) / Internetbrowser	Der Angreifer nutzt gängige Übermittlungsmechanismen (z. B. über unsichere Webseiten), um bekannte Malware (z. B. Malware, deren Existenz bekannt ist) in Informationssysteme von Unternehmen zu installieren/einzuschleusen.
1.5	Falscher Umgang mit kritischen und/oder sensiblen Informationen durch autorisierte Benutzer / Smartphone	Ein autorisierter, privilegierter Benutzer gibt versehentlich kritische/sensible Informationen über sein Smartphone preis.
1.6	Spear-Phishing (z.B. durch personalisierte Mails) / Mailsystem	Der Angreifer fälscht Mitteilungen von einer legitimen/vertrauenswürdigen Quelle, um sensible Informationen wie Benutzernamen, Kennwörter oder SSN zu erlangen. Typische Angriffe erfolgen über E-Mail, Instant Messaging oder vergleichbare Mittel.
1.7	Verwendung von nicht autorisierter Hard- und Software von Drittanbietern / Mitarbeitende	Dieses Risiko entsteht, wenn Mitarbeitende Geräte, Anwendungen oder Dienste in das Unternehmensnetzwerk einbringen, die nicht durch die IT-Abteilung geprüft und genehmigt wurden.
1.8	Social Engineering Angriffe, um Mitarbeitende davon zu überzeugen, schädliche Maßnahmen zu ergreifen (z.B. durch Shoulder Surfing) / Mitarbeitende	Der Angreifer unternimmt Aktionen (z. B. per E-Mail oder Telefon) mit der Absicht, Mitarbeitende überreden oder auf andere Weise dazu zu bringen, kritische/sensible Informationen (z. B. personenbezogene Daten) preiszugeben.
1.9	Verbreiten sensibler Informationen (z.B. durch Kommunikation über WhatsApp) / Instant-Messenger	Ein autorisierter Benutzer kontaminiert irrtümlich ein Gerät, Informationssystem oder Netzwerk, indem er darauf Informationen mit einer Klassifizierung/Sensibilität, zu deren Handhabung er nicht berechtigt ist. Die Informationen sind dem Zugriff Unbefugter ausgesetzt, und das Gerät, System oder Netzwerk ist nicht verfügbar, während der Schaden untersucht und entschärft wird.
1.10	Autorisiertem Personal folgen, um Zutritt zu organisatorischen Einrichtungen zu erhalten / Mitarbeitende / Physische Parameter	Der Angreifer folgt ("tailgates") autorisierten Personen in sichere/kontrollierte Bereiche mit dem Ziel, sich unter Umgehung der physischen Sicherheitskontrollen Zugang zu Einrichtungen zu verschaffen.

Kompetenzforschung und dessen Potential: – Ganzheitliche IT-Sicherheitsstrategie je Domäne

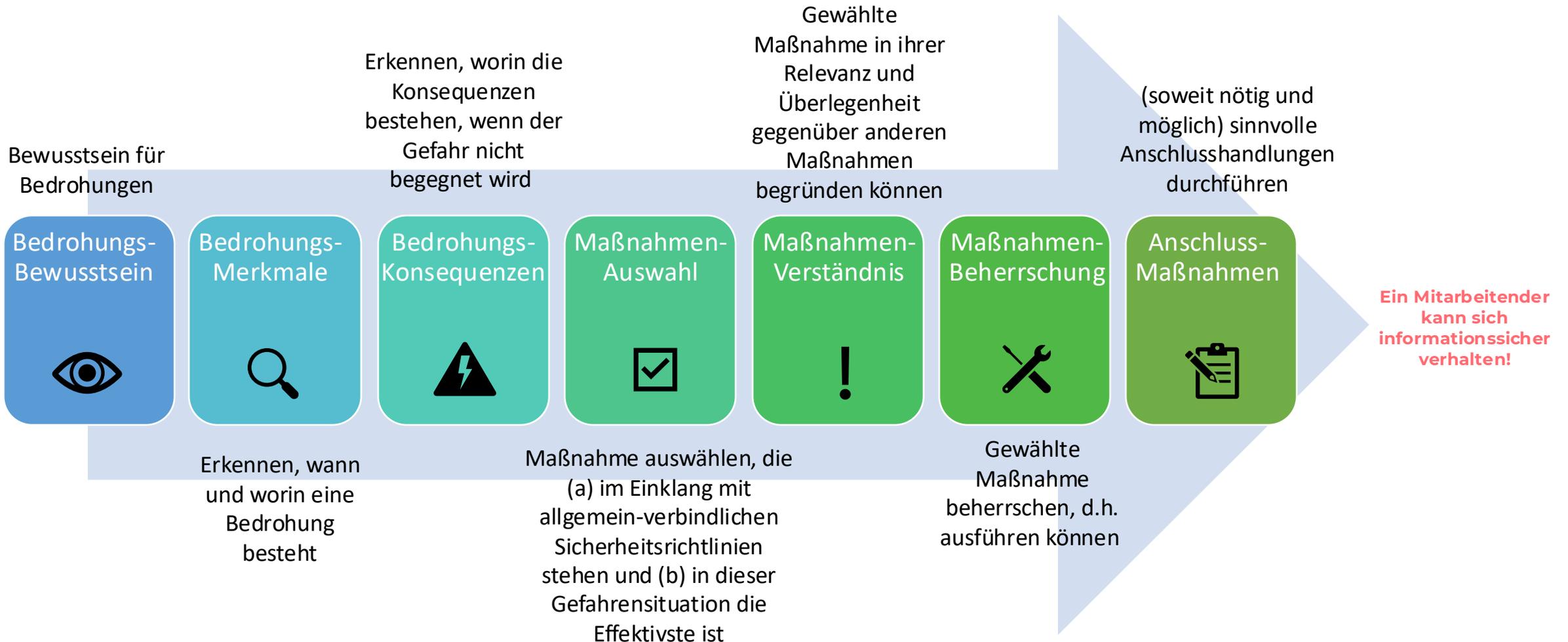
Jemand ist in einem Bereich **gut qualifiziert** durch:



Jemand ist **gut qualifiziert** sich informationssicher zu verhalten:



Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal





BAUSTEIN 2: KOMPETENZ-MESSUNG

Messung des IST-Zustands und Vergleich mit dem Soll-Zustand der Security Awareness

1.

Ergebnis: Kompetenz-Anforderungen

• Rolle: Ärztin / Arzt

Kompetenz-Linie

- Identity and Access
- Email use
- Internet use
- Incident reporting
- Mobile computing
- Information handling
- Social networking site (SNS) use

Kritische Assets

Informations-Assets	Operationsdaten, Diagnosen, usw.
Software-Assets	KIS, Patientenportal, usw.
IT-Assets	Laptop, Smartphones, Stations-PC, usw.
Zugänge	Operationssaal, usw.
Zentrale Bedrohungsvektoren	

2.

Sie sind derzeit für einen Patienten zuständig, auf dessen Blutprobe Sie schon den ganzen Tag warten, um die medikamentöse Einstellung vorzunehmen und dem Stationsarzt, Herrn Köhler, mitzuteilen.

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informationssicherheit** der Universitätsklinik Grüning?

Sortieren Sie nach folgendem Schema:

[1] Die Situation ist **am** bedrohlichsten.

[2] Die Situation ist **weniger** bedrohlich.

[3] Die Situation ist **am wenigsten** bedrohlich.



Hallo Herr Köhler,

Hier ist das Testergebnis der Blutprobe von Herrn John Doe, 01.03.1970.

Nüchternblutzucker: 215 mg/dL
Zielbereich: 70-130 mg/dL
Hämoglobin-A1C: 8,9%
Zielbereich: < 7.0 %

15:38

Die Ergebnisse deuten auf eine unzureichend kontrollierte Diabetes hin. Wir müssen möglicherweise die Medikamentenpläne und/oder den Lebensstil des Patienten ändern, um den Blutzuckerspiegel und den Hämoglobin-A1C-Wert zu senken.

15:39

Hallo Herr Köhler,

Hier ist das Testergebnis der Blutprobe von JD, 1970.

Nüchternblutzucker: 215 mg/dL
Zielbereich: 70-130 mg/dL
Hämoglobin-A1C: 8,9%
Zielbereich: < 7.0 %

15:38

Die Ergebnisse deuten auf eine unzureichend kontrollierte Diabetes hin. Wir müssen möglicherweise die Medikamentenpläne und/oder den Lebensstil des Patienten ändern, um den Blutzuckerspiegel und den Hämoglobin-A1C-Wert zu senken.

15:39

Hallo Herr Köhler,

Die Testergebnisse der Blutprobe unseres Patienten sind da. Die Ergebnisse deuten auf eine unzureichend kontrollierte Diabetes hin. Wir müssen möglicherweise die Medikamentenpläne und/oder den Lebensstil des Patienten ändern, um den Blutzuckerspiegel und den Hämoglobin-A1C-Wert zu senken.

15:38



3.

<p>Social Engineering / Social Media Systeme</p> <p>Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.</p> <p>50%</p> <p>KOMPETENZDIMENSION</p> <ul style="list-style-type: none"> ▲ Threat Awareness ✓ Threat Identification ✓ Threat Impact Assessment ✗ Tactic Choice ✓ Tactic Justification ✗ Tactic Mastery ✗ Tactic Check & Follow-Up <p>EMPFEHLUNG</p> <p>Basierend auf den Ergebnissen aus Ihrem ITS-Kompetenztest könnte ein ITS-Training im Bereich Social Engineering ihre ITS-Kompetenzen verbessern.</p>	<p>Social Engineering / Instantmessenger</p> <p>Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.</p> <p>86%</p> <p>KOMPETENZDIMENSION</p> <ul style="list-style-type: none"> ✓ Threat Awareness ✗ Threat Identification ✓ Threat Impact Assessment ✓ Tactic Choice ✓ Tactic Justification ✓ Tactic Mastery ✓ Tactic Check & Follow-Up <p>EMPFEHLUNG</p> <p>Basierend auf den Ergebnissen aus Ihrem ITS-Kompetenztest benötigen Sie kein Training im Bereich Social Engineering</p>
--	---

A	Personenbezogene Daten des Patienten werden nicht anonymisiert. (1)
B	Personenbezogene Daten des Patienten werden über WhatsApp ausgetauscht. (2)
C	Personenbezogene Daten des Patienten werden nicht pseudonymisiert. (1)
D	Der Nüchternblutzuckerspiegel liegt deutlich über dem Zielbereich. (0)



BEISPIEL: MESSINSTRUMENT

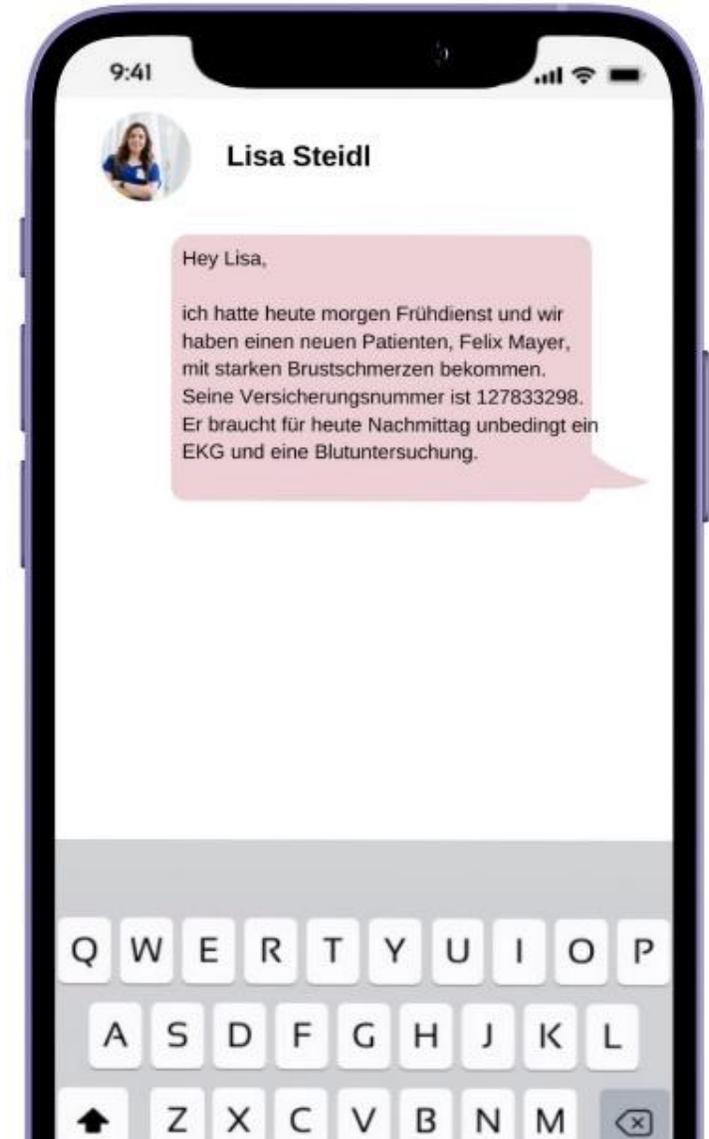
Messung des IST-Zustands der Security Awareness

Bitte betrachten Sie nochmals **diese Nachricht** genauer:

Was macht diese Nachricht konkret zu einer **Bedrohung der Informationssicherheit**?

Wählen Sie **eine** Antwort aus.

- Personenbezogene Daten des Patienten werden nicht anonymisiert.
- Personenbezogene Daten des Patienten werden über private Messengerdienste ausgetauscht.
- Personenbezogene Daten des Patienten werden nicht pseudonymisiert.
- Personenbezogene Daten des Patienten werden nicht mit einer Ende-zu-Ende-Verschlüsselung ausgetauscht.
- Der Patient hat starke Brustschmerzen und braucht für heute Nachmittag ein EKG.





BEISPIEL: MESSINSTRUMENT

Messung des IST-Zustands der Security Awareness

eCampusMail E-Mail Adressbuch Einstellungen

Zurück Schreiben Antworten Allen antwor... Weiterleiten Löschen Verschieben Drucken Markieren Mehr

Posteingang 16

Entwürfe

Gesendet

Spam

Gelöscht 1

Archives

Templates

Ideenwettbewerb 2020 Nachricht 10 von 1600

Von **ideenwettbewerb@gmail.com**

Absender

An **maxiluca.muster@stud.uni-goettingen.de**

Datum 2019-10-21 13:00

Anhang

Liebe Studenten!

Alle Studierenden sind herzlich eingeladen, mit guten Ideen und innovativen Vorschlägen am Ideenwettbewerb teilzunehmen. Gefragt sind Konzepte und Ideen zu positiven Veränderungen rund um das Motto in Studium und Lehre. Die besten Vorschläge werden mit bis zu **1.000 Euro** prämiert; **Einsendeschluss: 17. Februar 2020 (23.59 Uhr)**.

Ob als Einzelperson oder im Team – erläutern Sie Ihren Vorschlag und melden sich mit Ihrem Nutzer Account und Ihren Ideen einfach an:
<http://pstd.de/www.uni-goettingen/ideenwettbewerb/de>

Vielle Grüße
Hans Peltz

Georg-August-Universität Göttingen
Abt. Studium und Lehre
Wilhelmsplatz 2
D-37073 Göttingen
Tel. +49 (0) 551/39-113

- Absender = gmail.com
- Sprache – warum einloggen?
- Signatur = Rechtschreibfehler
- Link Wer-Bereich = pstd.de

Input Phishing



Stress

1. **Workload:** Erhöhter Arbeitsaufwand durch zusätzliche Mails
2. **Misstrauen:** Häufige und ohne Transparenz durchgeführte Simulationen werden als Manipulation wahrgenommen
3. **Technostress:** Stress durch bspw. Gamification

Bestrafung

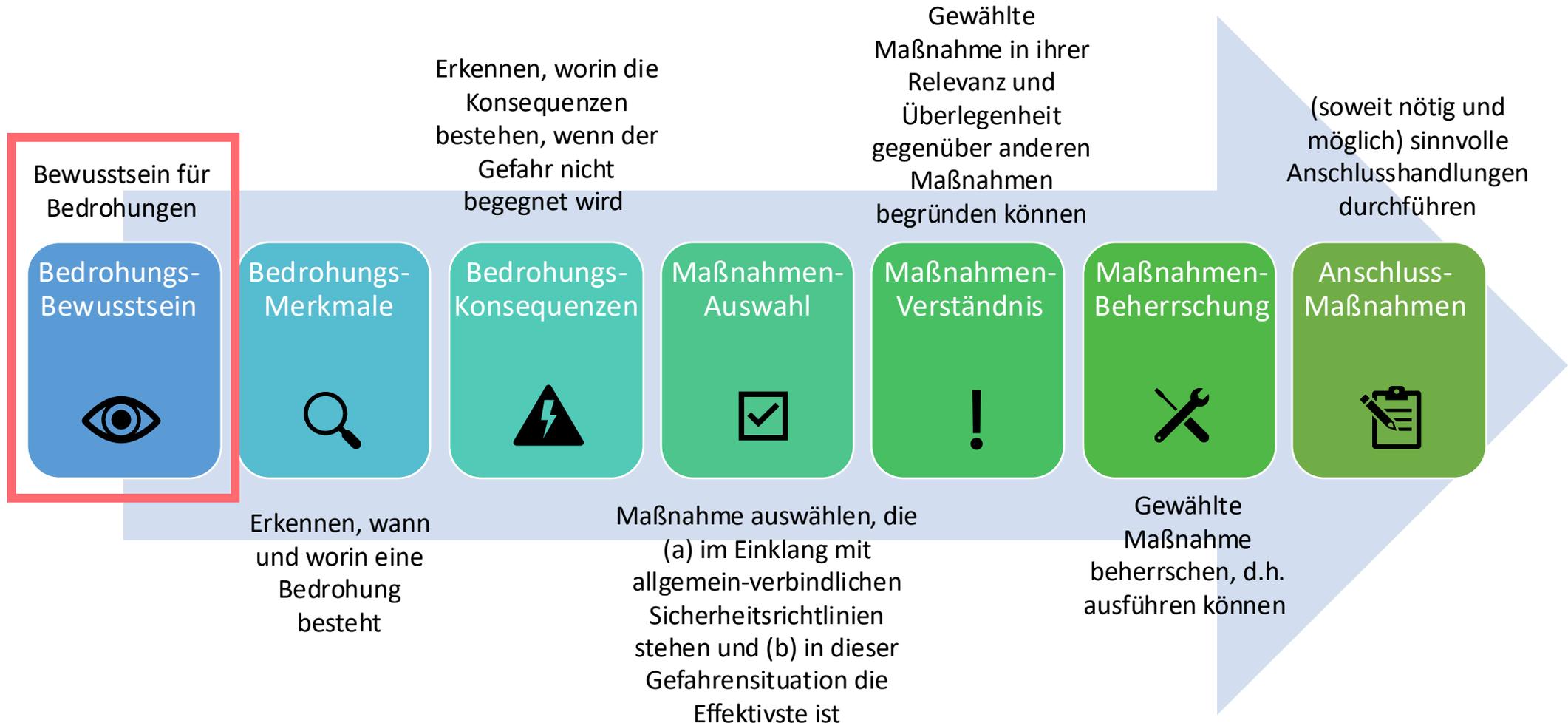
1. **Motivation:** Sinkende Motivation bspw. Phishingmails zu melden
2. **Lernbereitschaft:** Interesse an Situationen zu lernen sinkt stark
3. **Fehleranfälligkeit:** Mitarbeitende machen häufiger Fehler, die sie vorher nicht gemacht hätten

Messbarkeit

1. **Schwierigkeitsgrad:** Ohne Profizuordnung keine Aussagekraft
2. **Klickrate bei bestimmten Themen:** Keine Aussagekraft ohne vorherige Justierung
3. **Branchenvergleich:** Keine Aussagekraft, wenn Mails angepasst wurden

BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Bedrohungs-Bewusstsein – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Nachdem Sie heute Morgen Ihren Frühdienst beendet haben und nun zu Hause angekommen sind, erinnern Sie sich plötzlich daran, dass Sie während der Übergabe eine wichtige Information vergessen haben an Ihre Kollegin weitergegeben. Schnell zücken Sie Ihr privates Smartphone und senden eine kurze Nachricht über einen Ihrer privaten Messenger-Dienste an sie. Welche der folgenden möglichen Nachrichten ist die größte Bedrohung für die Informationssicherheit der Universitätsklinik Grüning?

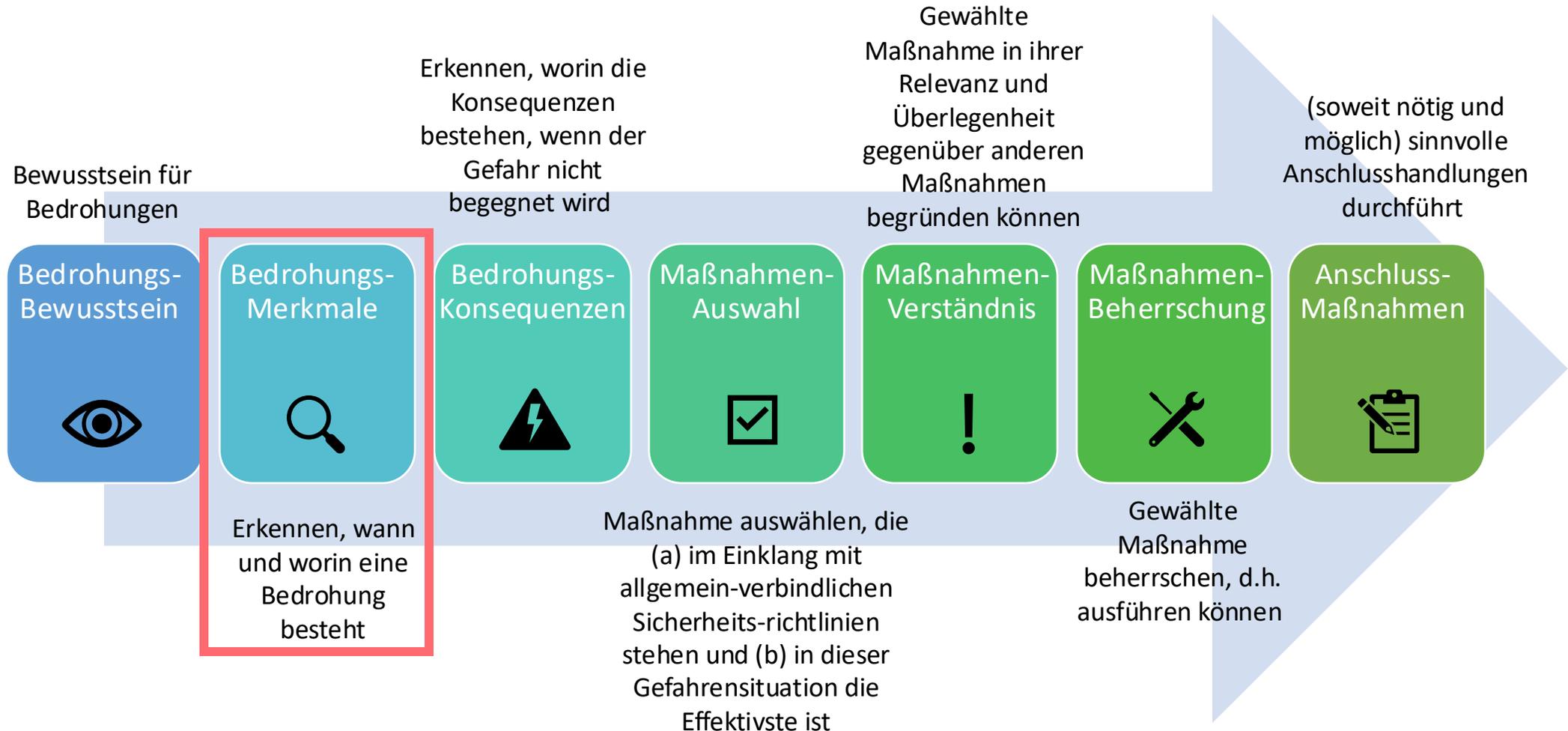
Sortieren Sie nach folgendem Schema:

- [1] Die Nachricht ist **am bedrohlichsten**.
- [2] Die Nachricht ist **weniger** bedrohlich.
- [3] Die Nachricht ist **am wenigsten** bedrohlich.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

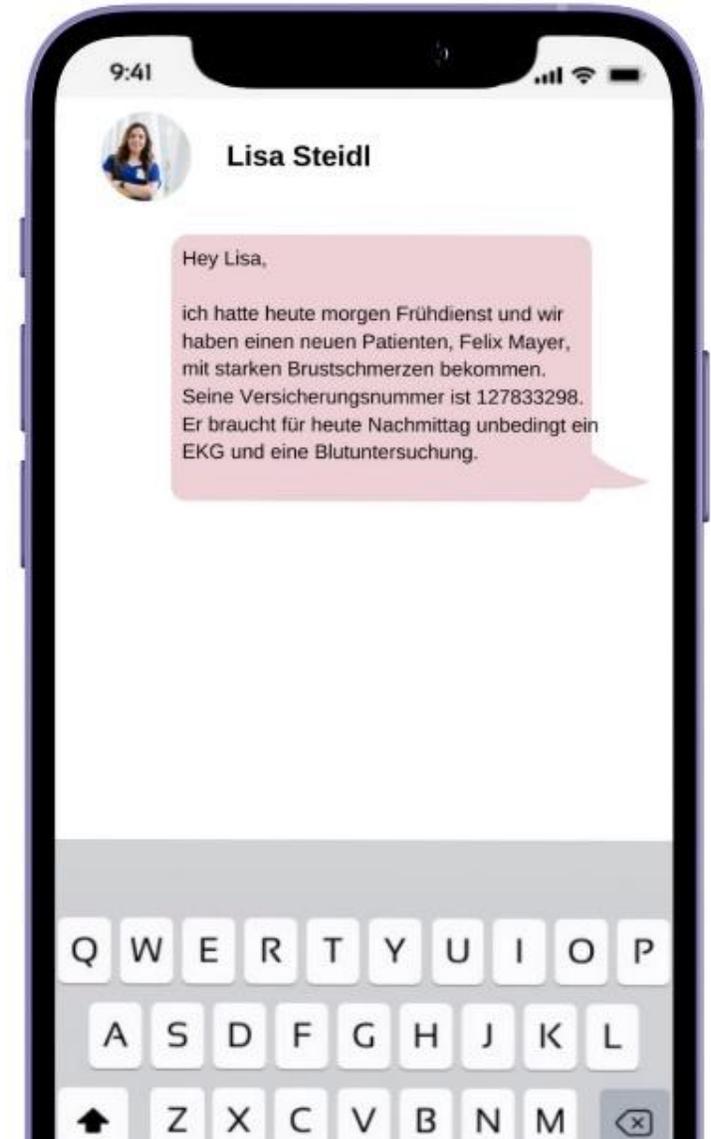
Bedrohungs-Merkmale – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Bitte betrachten Sie nochmals **diese Nachricht** genauer:

Was macht diese Nachricht konkret zu einer **Bedrohung der Informationssicherheit**?

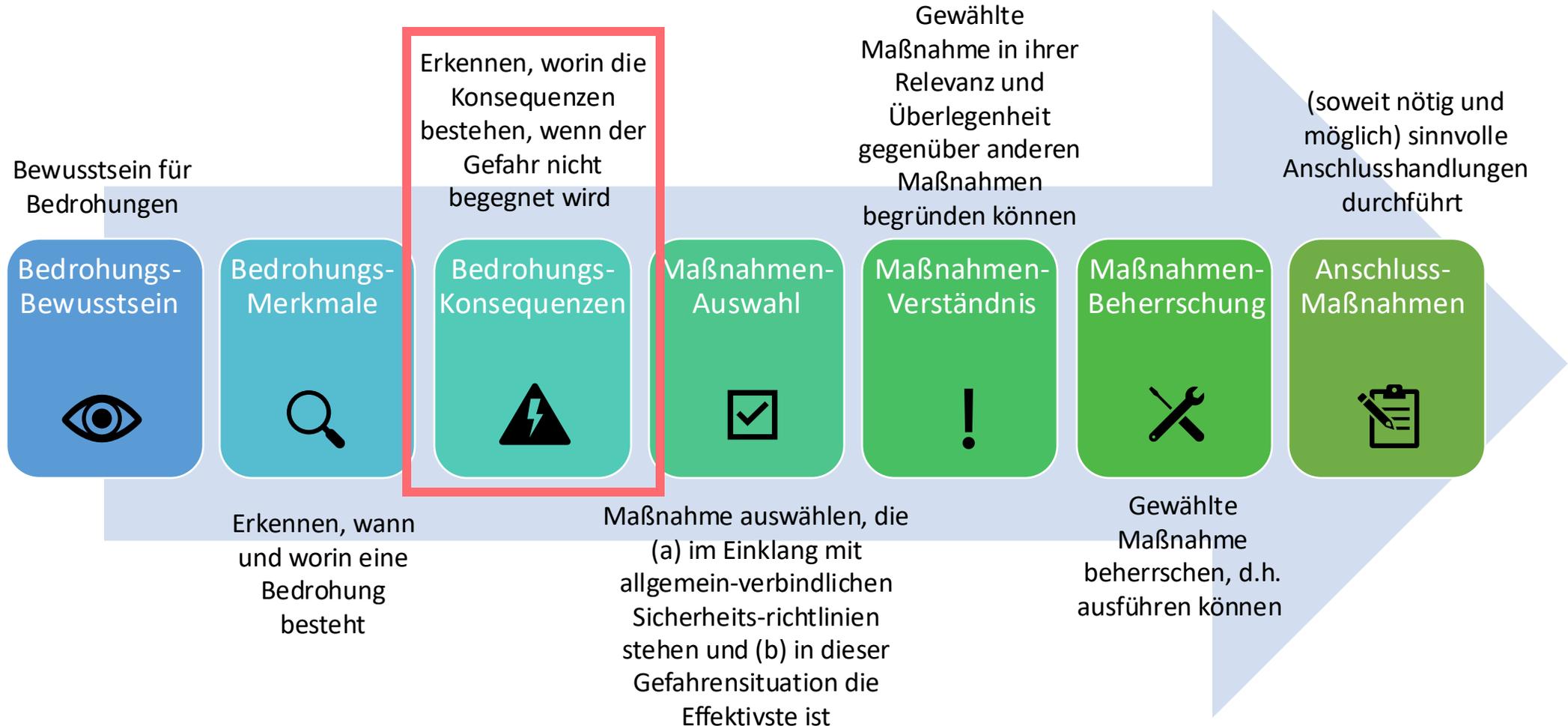
Wählen Sie **eine** Antwort aus.

- Personenbezogene Daten des Patienten werden nicht anonymisiert.
- Personenbezogene Daten des Patienten werden über private Messengerdienste ausgetauscht.
- Personenbezogene Daten des Patienten werden nicht pseudonymisiert.
- Personenbezogene Daten des Patienten werden nicht mit einer Ende-zu-Ende-Verschlüsselung ausgetauscht.
- Der Patient hat starke Brustschmerzen und braucht für heute Nachmittag ein EKG.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Bedrohungs-Konsequenzen – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche Konsequenzen könnte diese Nachricht schlimmstenfalls für die Informationssicherheit der Universitätsklinik Grüning nach sich ziehen?

Wählen Sie **eine** Antwort aus.

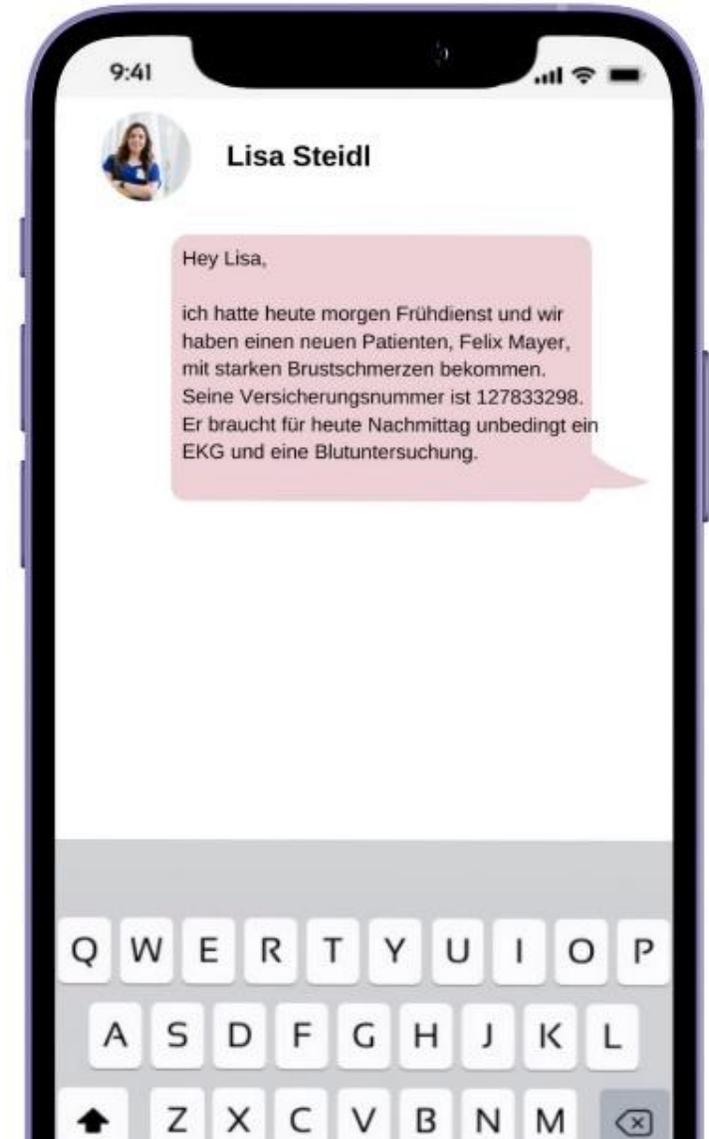
Durch diese Nachricht könnte ...

die Universitätsklinik Grüning eine Geldstrafe auferlegt bekommen.

es zu einer Verletzung des Datenschutzes führen, wenn der Patient die Weitergabe der personenbezogenen Daten ausdrücklich verbietet.

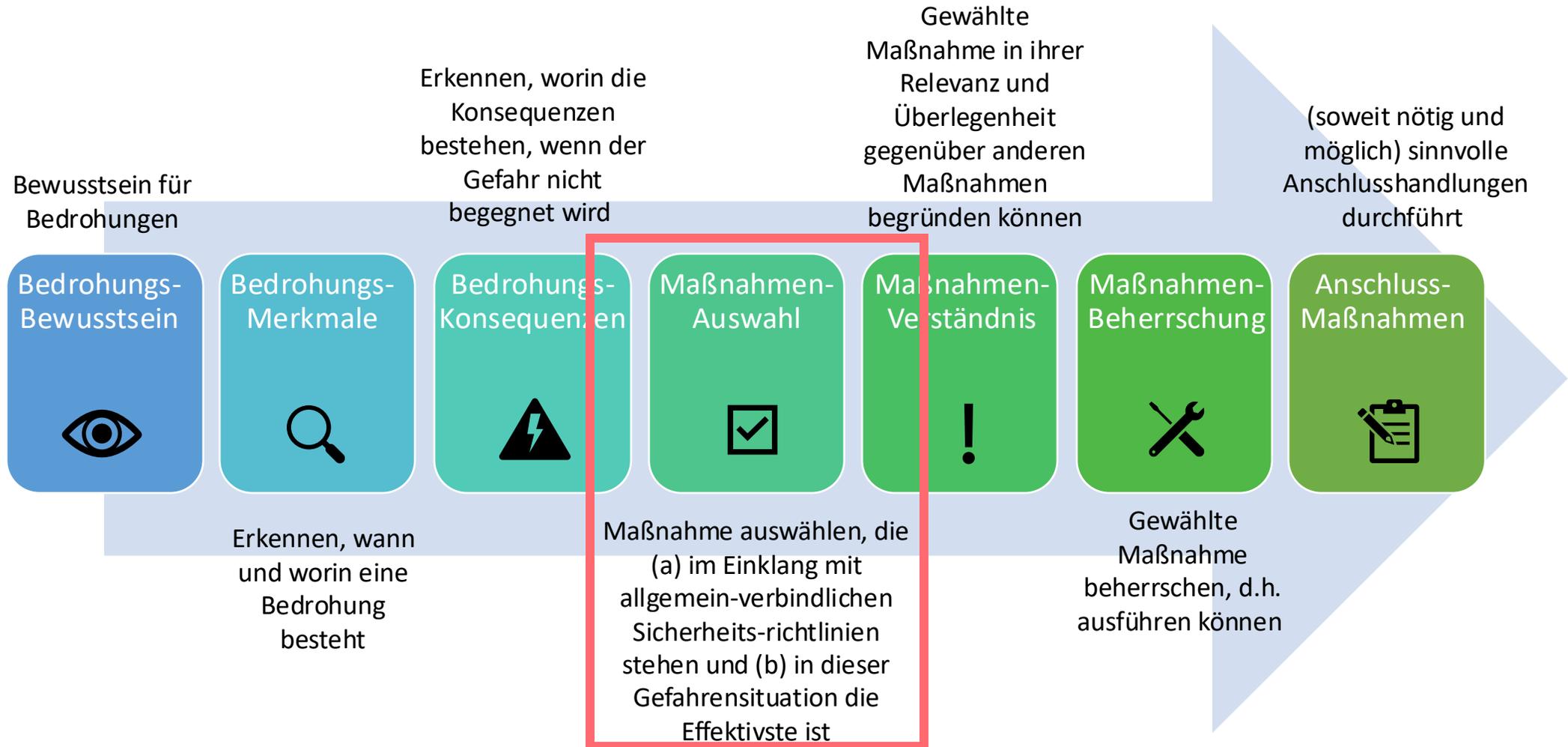
es die Privatsphäre des Patienten verletzen, was zu Rufschädigung des Patienten und Verlust des Vertrauens in das Personal der Klinik führen kann.

den beteiligten Mitarbeitenden der Universitätsklinik aufgrund von Datenschutzverletzungen ein Verlust ihres Arbeitsplatzes drohen.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

Maßnahmen-Auswahl – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche der aufgeführten **Maßnahmen** hätten Sie angesichts dieser Bedrohung ergreifen müssen?

Wählen Sie **eine** Antwort aus.

Ich übermittle personenbezogene Daten ...

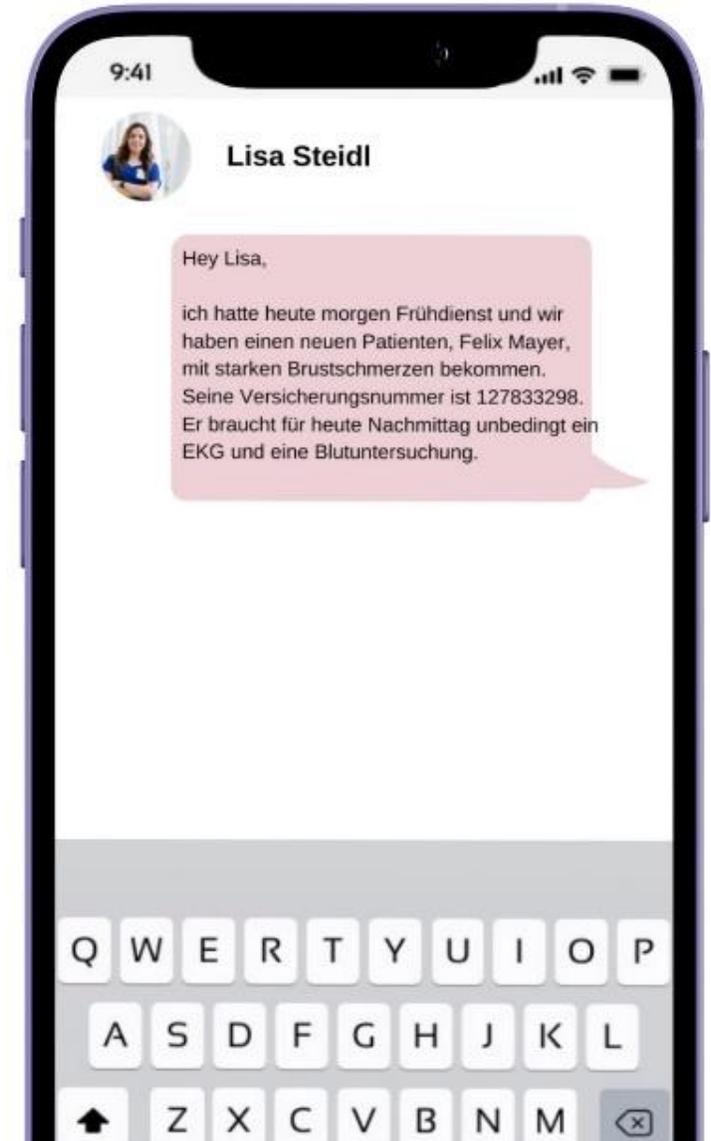
nur pseudonymisiert via private Messengerdienste.

nur anonymisiert via private Messengerdienste.

verschlüsselt über private Messengerdienste.

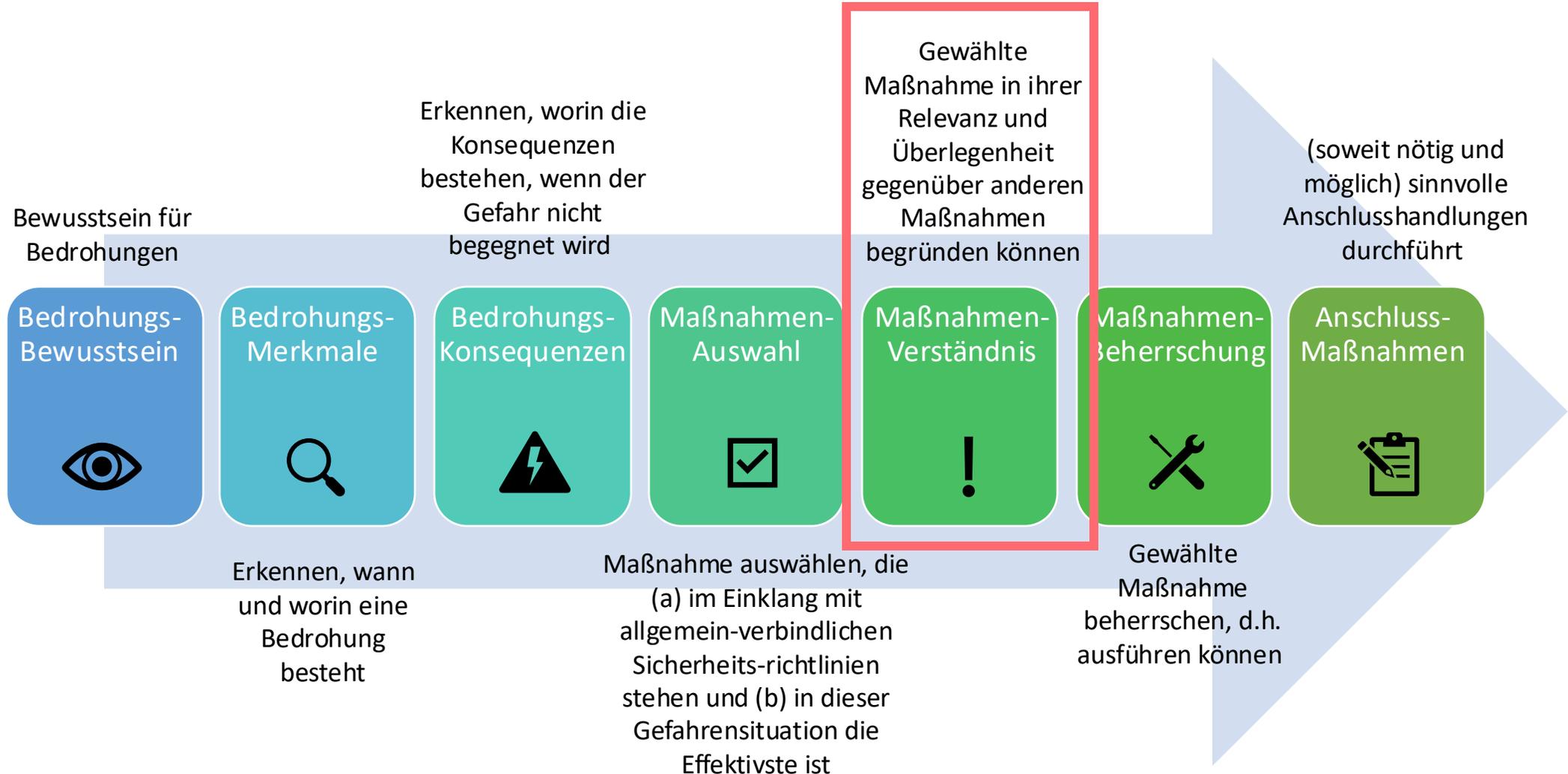
via private Messengerdienste und lösche die Nachricht sofort nachdem sie gelesen wurde.

über keinen meiner privaten Messengerdienste.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



BEISPIEL

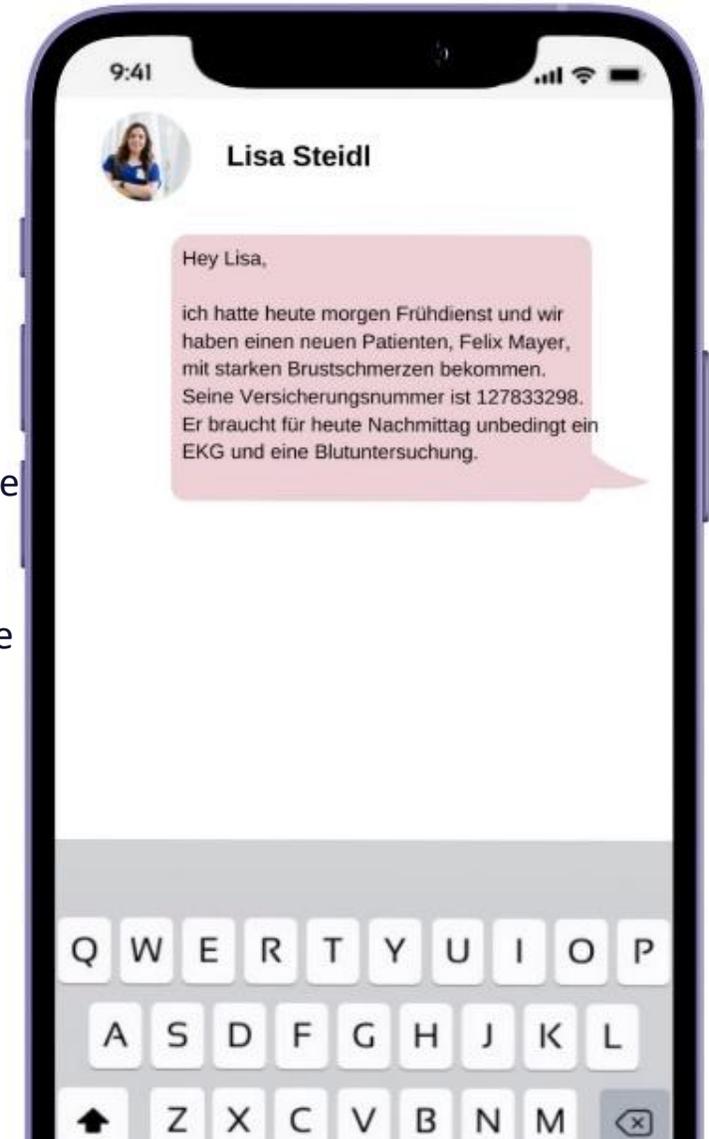
Maßnahmen-Verständnis – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Warum ist es wichtig, personenbezogene Daten über organisationsinterne Kommunikationswege zu übermitteln?

Wählen Sie **eine** Antwort aus.

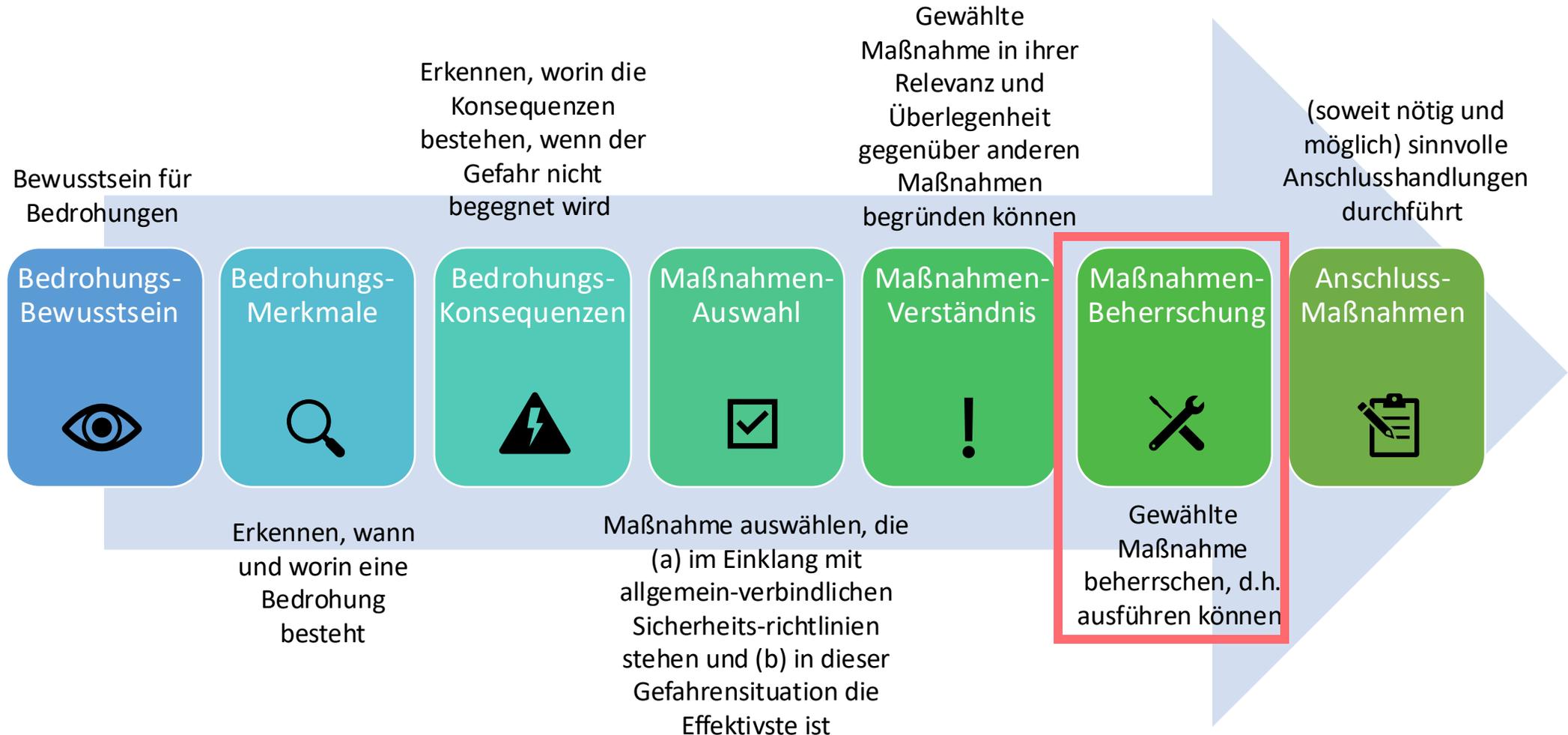
Diese Wege gewährleisten ...

- ... eine höhere Geschwindigkeit beim Übermitteln von Informationen und verbessern die Effizienz der medizinischen Versorgung.
- ... gewährleisten den Schutz personenbezogener Daten der Patient:innen, indem sie über notwendige Sicherheitsmaßnahmen verfügen.
- ... eine unverschlüsselte Übermittlung personenbezogener Daten, um unbefugten Zugriff und Datenlecks zu verhindern.
- ... eine bessere Koordination zwischen den verschiedenen Abteilungen und Fachkräften im Gesundheitswesen, was zu einer verbesserten Patientenversorgung führen kann.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



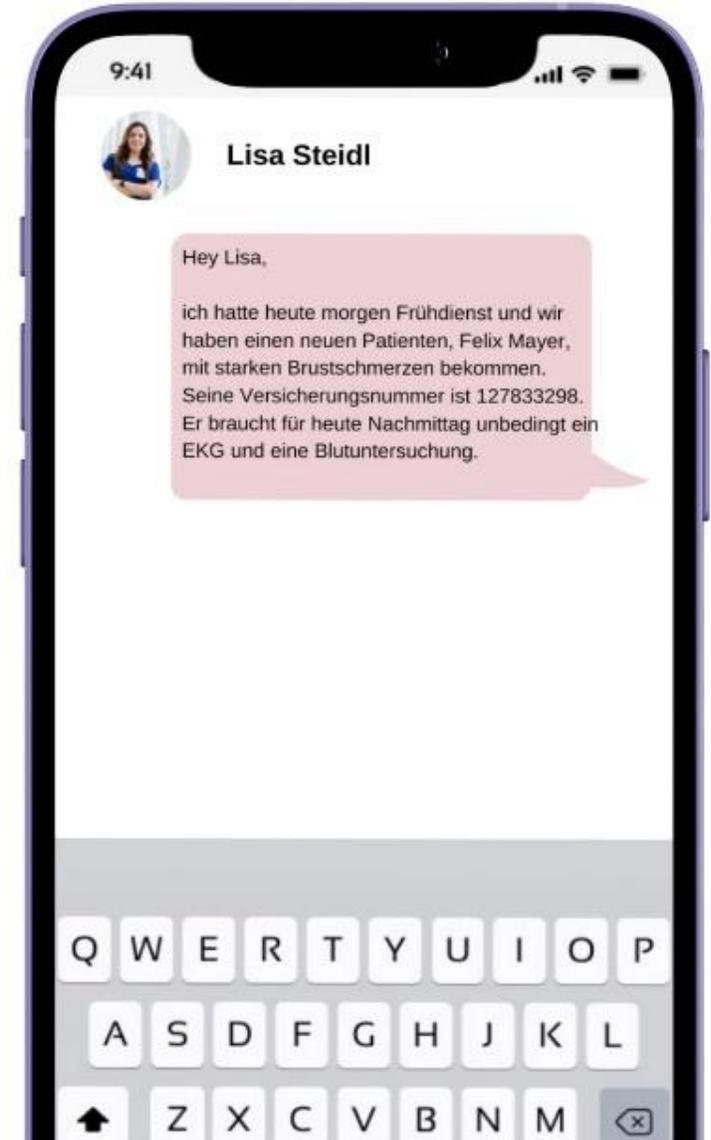
BEISPIEL

Maßnahmen-Beherrschung – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Wenn Sie personenbezogene Daten über organisationsinterne Kommunikationswege übermitteln möchten, **wie** gehen Sie dabei konkret vor?

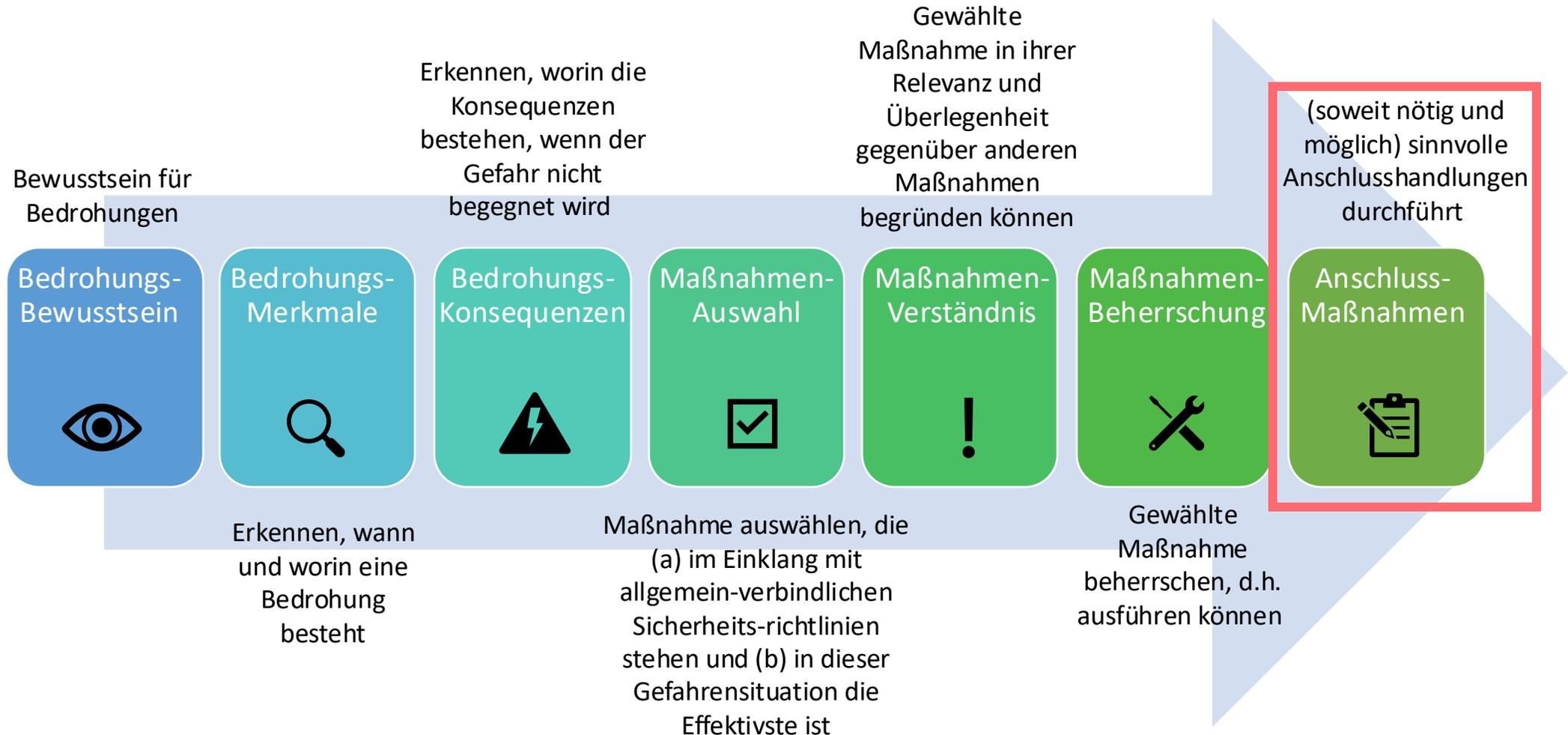
Wählen Sie **zwei** Antworten aus.

- Ich übermittle die Information unverschlüsselt über meine private E-Mail.
- Ich übermittle die Information vollständig über die klinischen IT-Systeme.
- Ich rufe meine Kollegin bei Dringlichkeit persönlich per Diensttelefon an und mache sie auf die Information aufmerksam.
- Ich übermittle die Information verschlüsselt über meine private E-Mail.
- Ich übermittle die Information über eine kurze SMS mit meinem privaten Smartphone.



BEISPIEL

Entwicklung Kompetenzmessinstrumente Profil : medizinisches Fachpersonal



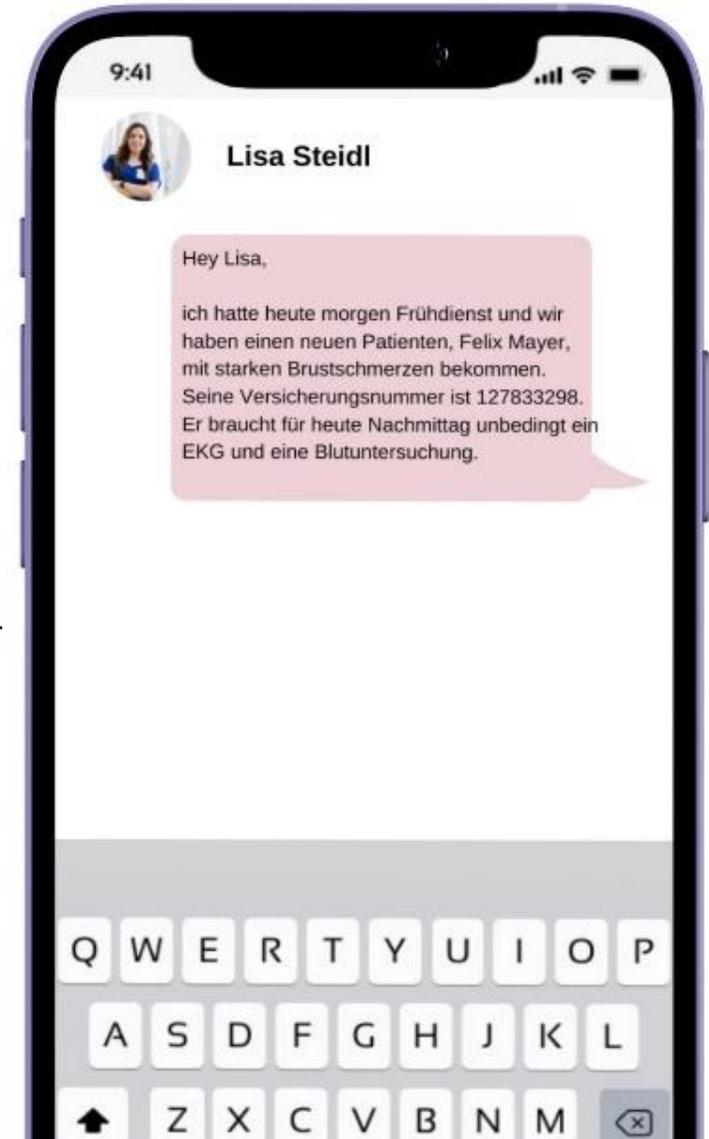
BEISPIEL

Anschluss-Maßnahmen – Entwicklung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Welche **ergänzenden Maßnahmen** zur Gefahrenabwehr sind in dieser Situation sinnvoll oder gar notwendig?

Wählen Sie **zwei** Antworten aus.

- Ich informiere mich über die aktuellen Datenschutzrichtlinien und -vorschriften meiner Organisation und halte mich daran.
- Ich beantrage die Nutzung von Ende-zu-Ende-Verschlüsselung für meine privaten Messenger-Dienste bei der Informationssicherheitsabteilung.
- Ich nehme regelmäßig an Schulungen und Fortbildungen zum Datenschutz und zur Datensicherheit teil.
- Ich anonymisiere alle personenbezogenen Daten während der Kommunikation mit meiner Kollegin.



Steigerung der Trainingsmotivation durch situierte, tätigkeits-adäquate und interaktive Trainings-Module



Leitfrage: Wie lassen sich effektiv und tätigkeits-adäquat die benötigten Kompetenzen vermitteln?

Ergebnis

- Interaktive-Online-Trainings („Micro-Interventionen“)
- Situiert, ausgelegt an beobachteten Handlungsszenarien
- Kurzweilig, leicht in den Arbeitsalltag integrierbar



BAUSTEIN 4: KOMPETENZ-ANWENDUNG

Nachhaltige Steigerung des tatsächlichen sicheren Verhaltens der MitarbeiterInnen im Arbeitsalltag

Poster

A4-1

Schütze deine Patienten und Daten
Mache mit dem IT-Sicherheitstraining und werde zum Helden der Datensicherheit. Melde dich heute noch an!

Selbstwirksamkeit, Identität
Dieser Nudge setzt auf die Verantwortung (self-efficacy) und Identifikation (identity theory) der Mitarbeiter als Beschützer der Patienten und Daten. Durch die Verwendung des Wortes "Helden" wird eine positive Assoziation und eine soziale Norm geschaffen, die die Mitarbeiter dazu motivieren soll, am Training teilzunehmen.

A4-2

Deine Entscheidung zählt
Stärke die Sicherheit unserer Klinik – nimm am IT-Sicherheitstraining teil! Anmeldung im Intranet oder bei der IT-Abteilung

Autonomie (Perceived Locus of Control), Reaktanz
Dieser Nudge betont die Entscheidungsgewalt der Mitarbeiter und zeigt, dass ihre Entscheidung einen direkten Einfluss auf die Sicherheit der Klinik hat. Das Gefühl der Autonomie bewirkt, dass Mitarbeiter eher bereit sind, sich für das Training anzumelden.

A4-3

Werde Teil des Sicherheitsteams
Gemeinsam können wir Hackerangriffe abwehren. Melde dich für das IT-Sicherheitstraining an und unterstütze unser Team!

Social belonging
Dieser Nudge setzt auf sozialen Zusammenhalt und Teamgeist. Mitarbeiter sollen das Gefühl bekommen, dass sie Teil eines größeren Ganzen sind und gemeinsam zur Sicherheit der Klinik beitragen können.

Leitfrage: Wie lässt sich die ‚Knowledge-Doing-Gap‘ umschiffen?

Ergebnis

- Micro-Nudges: Aufsteller, Bildschirmschoner, Innovative Konzepte „Micro-Games“
- Kampagnen-Pläne

Innovative Konzepte



Aufsteller





Testung Kompetenzmessinstrumente Profil: medizinisches Fachpersonal

Die Messauswertungen zeigen, dass die spezifischen Trainings einen signifikant höheren Lerneffekt haben, als allgemeine Trainings.

Ich empfand das Thema als spannend und wichtig. Wenn ich was verbessern müsste: eine Fortschrittsanzeige ;)

Das waren realistische Situationen, die passieren können, besonders die erste. Die Studie hat auch Spaß gemacht zu bearbeiten und zu überlegen, wie ich in der Situation reagieren würde.

Sehr immersiv und extremst realistische Situationen. Zudem auch tolle Bilder!

ich musste teilweise raten, weil ich nicht sicher war

Ein abschließendes Feedback, dass die gewählten Antworten noch einmal mit den korrekten Maßnahmen vergleicht, wäre wünschenswert gewesen.

Die Teilnahme per Mobiltelefon war teilweise schwierig. Die drei Situationen, welche ein Rechnungssystem zeigten und Detailansichten der Rechnungen war auch in Vergrößerung so gut wie nicht zu lesen. Evtl zukünftig auf PC beschränken?



Vielen Dank für Ihre Aufmerksamkeit!

**Vielen Dank für Ihre
Aufmerksamkeit!**

LinkedIn



Dr. Kristin Masuch



KISK-Materialien



Kontakt

kristin.masuch@cysec-
institut.de

ITS.kompetent- Materialien

