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

Allgemeine Hinweise zu den stellenspezifischen Kampagnenplänen

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Kampagnenziel:

Unser Vorgehensmodell für IT-Sicherheit (ITS) (
Abbildung 1: ITS-Vorgehensmodell
) beschreibt einen systematischen Ansatz zur Förderung der ITS-Kompetenzen Ihrer Mitarbeitenden im Krankenhaus. Zunächst wird die Belegschaft anhand spezifischer (1) ITS-Anforderungsprofile klassifiziert. Diese Profile definieren die notwendigen Fähigkeiten und Fertigkeiten, die für verschiedene Rollen und Aufgaben im Bereich der Informationssicherheit erforderlich sind und ermöglichen eine gezielte Identifikation der Schulungs- und Entwicklungsbedarfe (SOLL). Der Handlungsbedarf wird anschließend mit unseren (2) ITS-Kompetenztests ermittelt (IST). Diese Tests bewerten die Fähigkeiten und Fertigkeiten der Belegschaft in Bezug auf Informationssicherheit. Die Ergebnisse der Kompetenztests helfen dabei, spezifische Bereiche zu identifizieren, in denen die Mitarbeitenden zusätzliche Schulungen benötigen, um den Anforderungen gerecht zu werden. Wenn die Kompetenztests einen hohen Handlungsbedarf aufzeigen, werden im dritten Schritt gezielte (3) ITS-Trainings durchgeführt. Diese Schulungen zielen darauf ab, die festgestellten Defizite zu beheben und die ITS-Kompetenzen der Beschäftigten zu fördern. Um das ITS-Bewusstsein dauerhaft auf einem hohen Niveau zu halten, werden schließlich (4) ITS-Nudges eingesetzt. Diese Nudges sind subtile Hinweise und Anreize, die das Verhalten der Mitarbeitenden positiv beeinflussen, ohne Zwang auszuüben. Diese Maßnahmen fördern kontinuierlich das Bewusstsein für Informationssicherheit und unterstützen die Belegschaft dabei, dauerhaft sicherheitsbewusst zu handeln.

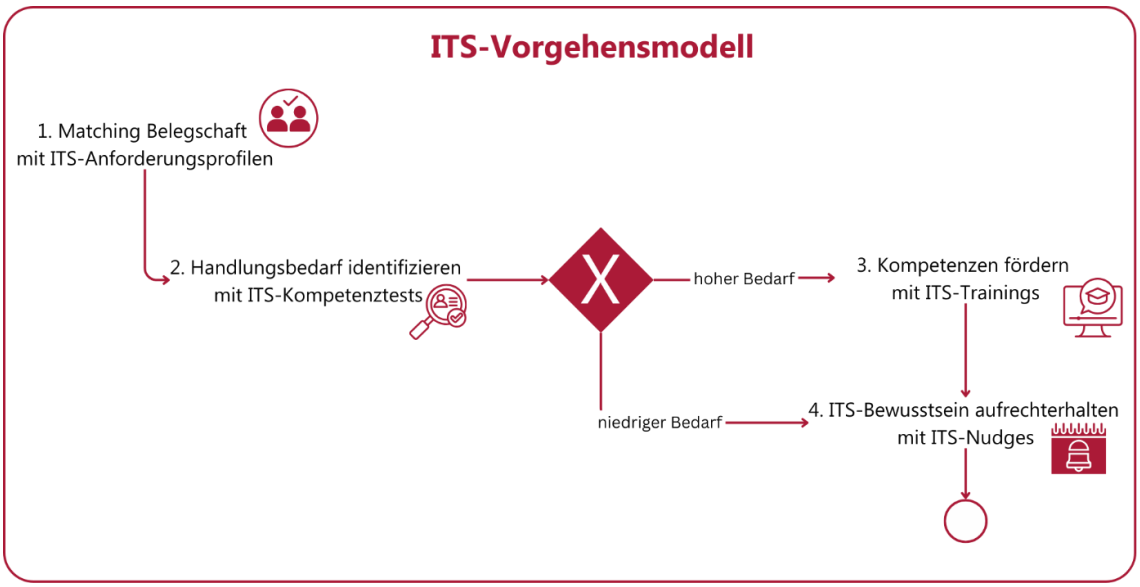

Abbildung 1: ITS-Vorgehensmodell

1.1 Matching Belegschaft mit ITS-Anforderungsprofilen

Zielsetzung: Die Belegschaft wird anhand unserer ITS-Anforderungsprofile klassifiziert und mit stellenprofilspezifischen Bedrohungsvektoren konfrontiert.

Die Vermittlung von ITS-Kompetenzen ist abhängig von der jeweiligen Stelle, welche die einzelnen Mitarbeitenden innehaben. In Abhängigkeit von den im Arbeitsalltag relevanten Bedrohungsbereichen bzw. der genutzten, vulnerablen Assets (z. B. Mobiltelefon, Laptop, Drucker) können Bedrohungsereignisse (z. B. Phishing, Ransomware, DDoS-Attacke) mit einer unterschiedlich hohen Wahrscheinlichkeit auftreten. Daher besteht das vorrangige Ziel dieses Kampagnenplans darin, den Soll-Bedarf an notwendigen ITS-Kompetenzen stellen- bzw. anforderungsprofilspezifisch aufzuzeigen. Um eine passende Zuordnung der einzelnen Beschäftigten zu einem passenden Anforderungsprofil zu ermöglichen, werden die zu prüfenden Personen zunächst nach ihrem aktuellen Anteil des Patientenkontakts im Arbeitsalltag anhand einer 5-Punkt-Likertskala („viel Patientenkontakt“ <-> „wenig Patientenkontakt“) befragt (vgl. Abbildung 2). Beispielsweise ist davon auszugehen, dass Kinderärztinnen und Kinderärzte relativ langen und umfassenden Patientenkontakt aufweisen, wohingegen Radiologinnen und Radiologen angesichts umfassender technologischer Hilfsmittel im Vergleich einen geringeren Patientenkontakt aufweisen. Basierend darauf werden spezifische Testszenarien in das Testprogramm integriert, indem die jeweilige Anzahl an Testszenarien aus dem jeweiligen Bereich (d.h. Handlungssituation mit „viel Patientenkontakt“ vs. „wenig Patientenkontakt“) einbezogen werden. Diese Differenzierung gilt nicht nur für Stellenprofile im Bereich „Ärztliches Fachpersonal“, sondern auch „Medizinisches Fachpersonal“ und „Verwaltungsfachpersonal“. Ebenso Beschäftigte in der Verwaltung, die einen moderaten Patientenkontakt angeben (z.B. Patientenabrechnung), werden insbesondere mit Bedrohungsszenarien konfrontiert, die sich auf eher entsprechende Tätigkeiten in ihrem Arbeitsalltag beziehen. In diesem Zuge erhalten sie weniger Bedrohungsszenarien, die auf Patientenkontakt ausgerichtet sind. Im Gegensatz dazu werden bei Beschäftigten, die im Rahmen ihrer Selbsteinschätzung viel Patientenkontakt angeben, auch mehr Szenarien mit Bezug zum Patientenkontakt vorgeschlagen (z.B. im Falle der medizinischen Fachangestellten). So kann ein individuell zugeschnittenes Testprogramm für alle Beschäftigten geliefert werden.

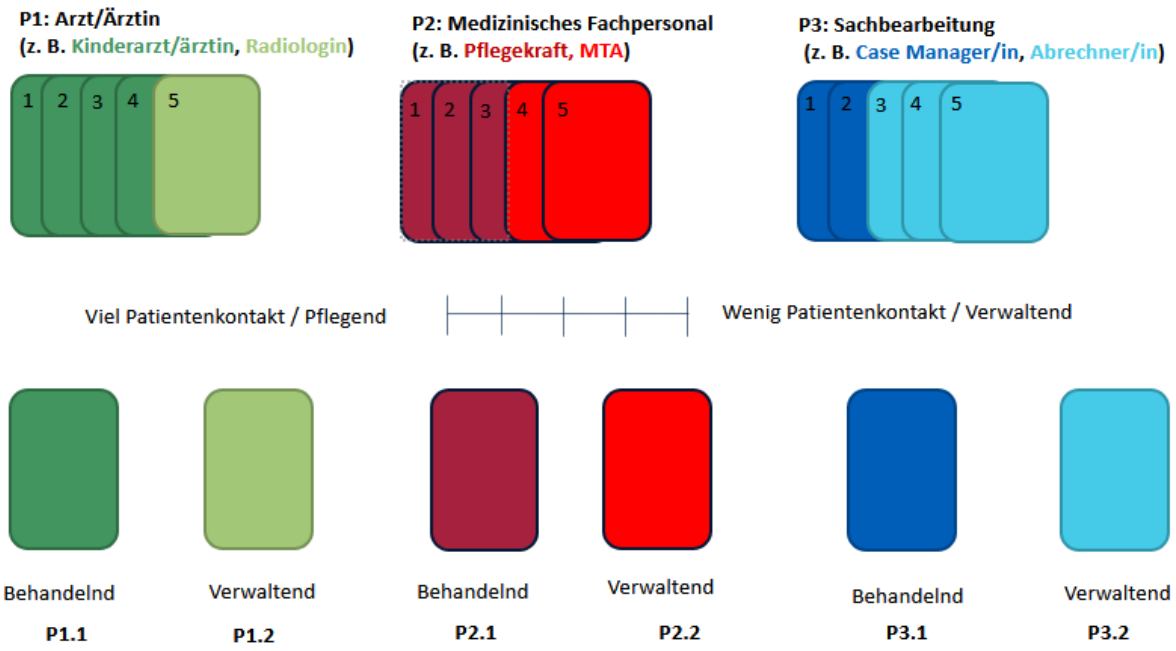

Abbildung 2: Differenzierung der ITS-Anforderungsprofile

Im Folgenden erfolgt eine Spezifizierung der drei übergeordneten Stellenprofile (1) „Ärztliches Fachpersonal“, (2) „Medizinisches Fachpersonal“ und (3) „Verwaltungsfachpersonal“ (

)

Abbildung 3: Differenzierung der übergeordneten ITS-Anforderungsprofile

Für die drei übergeordneten Anforderungsprofile (Ärztliches Fachpersonal, Medizinisches Fachpersonal und Verwaltungsfachpersonal) wurden sowohl **Bedrohungsbereiche** (**kritische Assets)** als auch **Bedrohungsereignisse** identifiziert, die gemeinsam jeweils einen **Bedrohungsvektor** bilden. In diesem Zusammenhang definieren wir als Bedrohungsbereich die möglichen Unternehmenswerte, die von verschiedenen Bedrohungsereignissen ins Visier genommen werden können. Beispiele für physische Unternehmenswerte sind Server, Laptops oder USB-Sticks, während non-physische Unternehmenswerte Social-Media-Netzwerke oder Buchhaltungssoftware sein können. Die zweite Dimension, das Bedrohungsereignis, umfasst Bedrohungsquellen, die potenziell Schaden an den zuvor erläuterten Bedrohungsbereichen verursachen können. Mögliche Bedrohungsereignisse können einer der vier Unterdimensionen zugeordnet werden, die von Blank und Gallagher (2012) beschrieben wurden: feindlich (z. B. Phishing- oder DDoS-Attacken), unbeabsichtigt (z. B. Weitergabe sensibler Informationen durch privilegierte Nutzer), strukturell (z. B. veraltete Displays) oder umweltbedingt (z. B. Brand oder Hochwasser). Abbildung 4 zeigt die Zusammensetzung eines Bedrohungsvektors durch ein Bedrohungsereignis und ein Bedrohungsbereich.

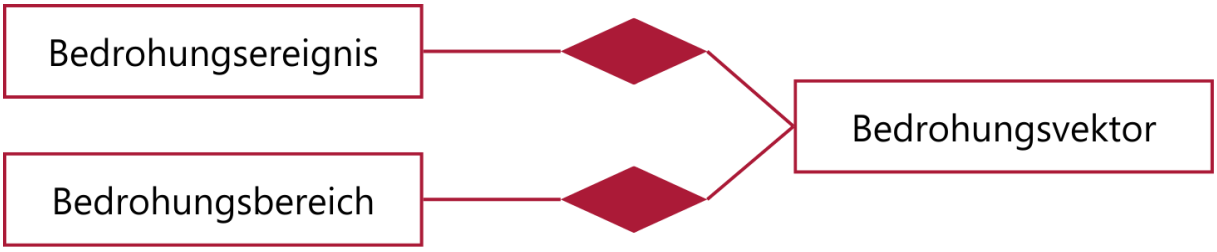

Abbildung 4: Zusammensetzung eines Bedrohungsvektors

1.2 Handlungsbedarf identifizieren mit ITS-Kompetenztests

Zielsetzung: Integration validierter ITS-Kompetenztests in das interne Lernmanagementsystem zur Erfassung und Analyse der ITS-Kompetenzen.

Für die Feststellung des stellenspezifischen Qualifizierungsbedarfs und der anschließenden adaptiven Zuweisung von ITS-Trainings nutzen Sie unsere Situational Judgement Tests, die darauf abzielen, die ITS-Kompetenzen Ihrer Mitarbeitenden zu unterschiedlichen Bedrohungsvektoren zu erfassen (IST-Stand) und zu bewerten. Das Testinstrumentarium zur Erfassung von ITS-Kompetenzen umfasst zehn Bedrohungssituationen pro Stellenprofil. Eine Bedrohungssituation besteht aus sieben Aufgaben und orientiert sich am Kompetenzstrukturmodell (Abbildung 5) bestehend aus sieben Kompetenzdimensionen, anhand dessen eine umfassende Bewertung von Fähigkeiten und Fertigkeiten möglich ist, die notwendig sind, um effektiv auf potenzielle Gefahren reagieren zu können. Das Modell dient dazu, sowohl die Wahrnehmung als auch die praktische Handhabung von Bedrohungen systematisch zu erfassen und zu verbessern.

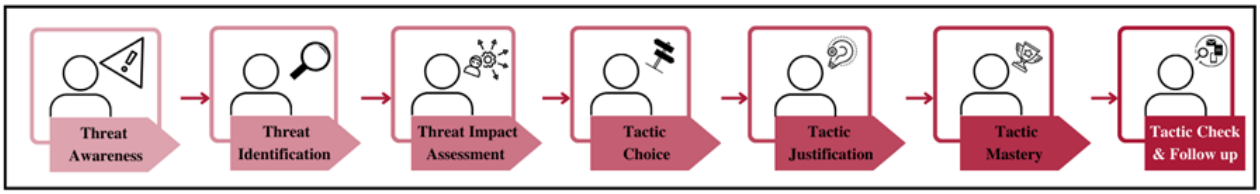

Abbildung 5: Kompetenzstrukturmodell

1. **Threat Awareness:** Lokalisierung von Gefahrenquellen in typischen Handlungssituationen des eigenen Stellenprofils
2. **Threat Identification:** Erkennen konkreter, konstitutiver Merkmale der Gefahrenquelle
3. **Threat Impact Assessment:** Abwägen/Bewerten der Konsequenzen des Nicht- oder / Fehlhandelns für Mitarbeitende & Organisation
4. **Tactic Choice:** Entscheidung über die ersten Schritte zur Gefahrenabwehr im eigenen Handlungs- /Verantwortungsbereich
5. **Tactic Justification:** Begründung der richtigen Maßnahme
6. **Tactic Mastery:** Realisierung/Durchführung der richtigen Maßnahme

7. **Tactic Check & Follow Up:** Ergänzende Maßnahmen zur Wirkungskontrolle (absichernd) oder Prävention (zukunftsorientiert)

Zur Integration der ITS-Kompetenztests in Ihr internes Lernmanagementsystem zur Erfassung und Analyse der ITS-Kompetenzen sind folgende Schritte notwendig:

Schritt 1: Bewertung der Kompatibilität

- Überprüfen Sie die vorhandenen ITS-Kompetenztests auf ihre inhaltliche Passung zu Ihrer Organisation.
- Passen Sie, wenn nötig, die Antwortoptionen und das Scoring der ITS-Kompetenztests an die spezifischen Bedürfnisse und Kontexte Ihrer Organisation an, ohne die Grundstruktur und den Testcharakter zu verändern.

Schritt 2: Technische Einrichtung

- Integrieren Sie die ITS-Kompetenztests technisch in Ihr Lernmanagementsystem unter Berücksichtigung der vorgenommenen Anpassungen.
- Stellen Sie sicher, dass die Tests innerhalb des Systems funktional und benutzerfreundlich sind.

Schritt 3: Datenerhebung und –Analyse

- Beachten Sie, dass jeder Bedrohungsvektor aus sieben Aufgaben besteht, die als Multiple-Choice (MC) oder Single-Choice (SC) Fragen formuliert sind. Jede Aufgabe ermöglicht das Erreichen von bis zu 2 Punkten, sodass insgesamt bis zu 14 Punkte pro Bedrohungsvektor erzielt werden können.
- Jede Bedrohungssituation dauert etwa 5-7 Minuten, was den Gesamtzeitaufwand geringhält und eine einfache Integration in den Arbeitsalltag ermöglicht.
- Nutzen Sie die vollautomatisierte Auswertung der Ergebnisse durch Ihr Umfragetool, um detaillierte Analysen der Kompetenzniveaus vorzunehmen und spezifische Stärken sowie Schwächen zu identifizieren.

Schritt 4: Auswertung und Qualifizierungsstrategieentwicklung

- Sammlung und Auswertung der Testergebnisse zur Identifikation individueller und kollektiver Kompetenzniveaus.

- Dokumentieren Sie den Qualifizierungsbedarf und weisen Sie in diesem Schritt gezielt Trainingsmaßnahmen (ITS-Trainings) zu, die auf die identifizierten Stärken und Schwächen abgestimmt sind.

Schritt 5: Evaluierung und Anpassung

- Bewertung der Wirksamkeit der Qualifizierungsmaßnahmen durch erneute Anwendung der Kompetenztests.

1.3 Kompetenzen fördern mit ITS-Trainings

Zielsetzung: Integration von ITS-Trainings in Form von kompetenzorientierten Erklärvideos im Lernmanagementsystem zur Förderung der ITS-Kompetenzen der Mitarbeiterinnen und Mitarbeiter.

Zum Kompetenzaufbau des für die einzelnen Stellenprofile relevanten Qualifizierungsbedarfs wurden je Stellenprofil sechs Trainingsvideos entwickelt. Die Auswahl und der Inhalt der Trainingsvideos leiten sich aus dem im Vorfeld identifizierten Qualifizierungsbedarf ab. Die Trainingsvideos orientieren sich an dem Kompetenzstrukturmodell (Abbildung 5), dessen Phasen in den Trainingsvideos durch farblich gestaltete Badges illustriert sind (Abbildung 6). Zu Beginn eines Trainings wird die erste Entwicklungsstufe „Einsteiger“, die die Kompetenzstufen Threat Awareness, Threat Identification und Threat Impact Assessment beinhaltet, durch ein rotes Badge dargestellt. Das rote Badge zeigt die Edukation des Basiswissens an. Hier wird angestrebt Kompetenzen zur grundlegenden Gefahrenerkennung und Sensibilisierung zu erreichen. Die zweite Entwicklungsstufe „Kenner“ wird durch ein gelbes Badge dargestellt und umfasst die Kompetenzstufen Tactic Choice, Tactic Justification und Tactic Mastery. Das gelbe Badge fokussiert weiterführende Kompetenzen zur eigenständigen Umsetzung von Sicherheitsmaßnahmen. Die dritte Entwicklungsstufe „Experte“ wird durch ein grünes Badge illustriert. Mit Abschluss des grünen Badges wurden alle Kompetenzen zur ganzheitlichen Risikoanalyse und zu Abwehrstrategien trainiert und aufgebaut. Diese Entwicklungsstufe beinhaltet die Kompetenzstufe Tactic Check & Follow Up.

Abbildung 6: Visualisierung der Entwicklungsstufen innerhalb eines Trainings

Die Trainingsvideos sind auf Deutsch verfügbar. Zudem wurden zwei Versionen erstellt, die jeweils mit deutschen und englischen Untertiteln versehen sind. Wie bei den Kompetenzmessinstrumenten müssen die Trainingsvideos in Ihr Lernmanagementsystem unter Berücksichtigung der Stellenprofile eingebettet werden. Dabei ist die Funktionalität und Benutzerfreundlichkeit der Trainingsvideos innerhalb des Lernmanagementsystems sicherzustellen. Ein Vorschlag zur zeitlichen und thematischen Reihenfolge der Bereitstellung

der Trainingsvideos für Ihre Mitarbeitenden kann dem stellenprofilspezifischen Kampagnenplan entnommen werden. Die empfohlene Reihenfolge leitet sich von dem Ziel ab, frühzeitig ein breites Wissen bei Ihren Mitarbeitenden aufzubauen und die meisten Bedrohungsvektoren zeitnah anzugehen. Diese Reihenfolge basiert auf einer Zuordnung der Trainingsvideos zu den jeweiligen Bedrohungsvektoren und folgt dem Prinzip „Vom Abstrakten zum Konkreten“. Dies bedeutet, dass zunächst Trainingsvideos priorisiert werden, die eine Vielzahl von Bedrohungsvektoren abdecken. Gleichzeitig werden Videos bevorzugt behandelt, die noch nicht adressierte Bedrohungsvektoren ansprechen.
Bitte beachten Sie, dass es sich bei dieser Reihenfolge um einen Vorschlag handelt, der das generische Ziel verfolgt, möglichst frühzeitig alle Bedrohungsvektoren zu adressieren und Kompetenzen aufzubauen. Abhängig von den in Ihrer Einrichtung im Vorfeld identifizierten Gefahren und dem Qualifizierungsbedarf kann von dieser Reihenfolge abgewichen werden.

Zeitliche Empfehlung

Gemäß der Anforderung aus dem B3S für Krankenhäuser (ANF – 0074) müssen Mitarbeiterinnen und Mitarbeitern regelmäßig – mindestens alle zwei Jahre – ITS-Schulungen angeboten werden. Gleichzeitig wird bei vergleichbaren Standards die Regelmäßigkeit auf einmal pro Jahr ausgelegt werden. Wir schlagen vor die Schulung innerhalb von 6 Monaten mit je einem Trainingsvideo pro Monat einzuplanen und dazwischen eine einjährige Pause.
Bitte überprüfen Sie, ob für Ihre Zertifizierungen alternative Zeiträume relevant sein könnten und ob die Trainings möglicherweise häufiger angesetzt werden sollten. Berücksichtigen Sie dabei auch saisonale Herausforderungen, wie zum Beispiel erhöhte Ausfallraten aufgrund von Krankheiten, Urlaubszeiten oder unvorhergesehenen Ereignissen, die die Teilnahme beeinträchtigen könnten. Eine vorausschauende Planung kann dabei helfen, Engpässe zu vermeiden und die Effizienz der Schulungsmaßnahmen sicherzustellen.

1.4 ITS-Bewusstsein aufrechterhalten mit ITS-Nudges

Zielsetzung: Einsatz und Implementation von ITS-Nudges in Form von situativen Alltagsnudges zur Schärfung eines allgemeinen ITS-Bewusstseins und zur Förderung poraktiver, sicherheitsbewusster Verhaltensweisen im Arbeitsalltag, um so die gesamte Sicherheitskultur im Krankenhaus zu stärken.

Unsere Alltagsnudges teilen sich in zwei Kategorien auf. Die Alltags-Nudges adressieren entweder konkrete Verstöße („In-Role“) oder den Aufbau einer Unternehmenskultur, die durch pro-soziale Verhalten („Extra-Role“) geprägt sein soll. Unter In-Role-Verhalten versteht man das Befolgen von expliziten Regeln und Vorschriften als Bestandteil des Jobs. Beispiele sind die Nichtweitergabe von Passwörtern, das Sperren von PCs oder einfach gesagt: die Einhaltung der geltenden Vorschriften. In-Role-Verhalten hängen in erster Linie von den Kompetenzen des Einzelnen ab. Extra-Role-Verhalten sind nicht über Vorschriften geregelt und und das Nichtbefolgen dieser Verhalten kann auch nicht bestraft werden. Beispiele für diese Art von Verhalten sind: das Helfen Anderer, freiwilliges Weitergeben von (ITS)- Wissen oder andere zu erinnern, sich vom PC abzumelden. Extra-Role-Verhalten sind gekennzeichnet durch Freiwilligkeit einerseits und Veranlagung anderseits. Die Motivation ist eine intrinsische.

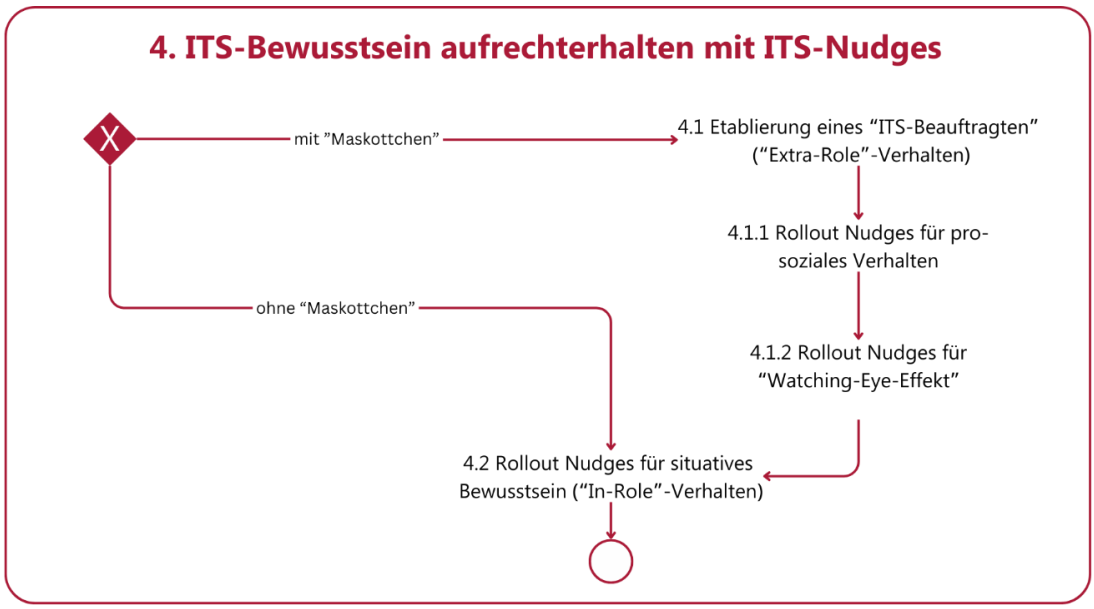

Abbildung 7: Vorgehensmodell ITS-Bewusstsein aufrechterhalten mit ITS-Nudges

Durch die Einführung des „SchutzFuchs“-Maskottchens etablieren Sie ein spielerisches und positives Belohnungssystem, das das ITS-Bewusstsein und prosoziales Verhalten im Krankenhaus fördert (4.1). Der SchutzFuchs wird als Botschafter für ITS im Krankenhaus

eingesetzt. Die Idee hinter diesem Ansatz ist es, durch den Einsatz eines Maskottchens ein höheres Bewusstsein und bessere Verhaltensweisen in Bezug auf ITS zu fördern. Dabei wird auf zwei verschiedene Rollen und Strategien gesetzt:

- **Extra-Role (4.1.1):**
    - **Belohnung von prosozialem ITS-Verhalten:** Besonders prosoziales Verhalten in Bezug auf ITS wird durch die Schenkung des SchutzFuchs-Maskottchens belohnt und anerkannt.
    - **Wettbewerbe und Gewinnspiele:** Es werden Wettbewerbe und Gewinnspiele etabliert, um zusätzlich eine extrinsische Motivation zu schaffen. Dies soll die Mitarbeitenden dazu anregen, sich aktiv und positiv mit ITS-Maßnahmen auseinanderzusetzen und diese in ihrem Alltag zu integrieren.
    - **Langfristige Assoziation:** Der SchutzFuchs wird langfristig von der Belegschaft mit ITS assoziiert.
    - **Strategische Platzierung:** Das Maskottchen (in Form von Stickern) wird an risikobehafteten Orten im Krankenhaus platziert, um die Assoziation zu nutzen und ein situatives Bewusstsein zu schaffen. Dies funktioniert ähnlich wie der „Watching-Eye-Effekt“, bei dem das Gefühl, beobachtet zu werden, sowohl prosoziales Verhalten als auch die Erinnerung an ITS fördert.

Die Nudging-Idee zielt darauf ab, durch subtile Hinweise und positive Verstärkung das Verhalten der Mitarbeitenden in Bezug auf ITS zu beeinflussen und nachhaltig zu verbessern. Der SchutzFuchs dient dabei als sichtbares und einprägsames Symbol für die Wichtigkeit von ITS und fördert ein bewusstes und verantwortungsvolles Verhalten im Umgang mit sensiblen Daten und IT-Systemen.

Vorgehensweise bei der Implementation des SchutzFuchs-Maskottchens:

- Entwickeln Sie ein Konzept für das SchutzFuchs-Maskottchen, das sowohl optisch ansprechend als auch repräsentativ für ITS ist. Definieren Sie die spezifischen Ziele, die Sie durch den Einsatz des Maskottchens erreichen möchten.

- Bestellen Sie das SchutzFuchs-Maskottchen für Wettbewerbe und Gewinnspiele.
- Informieren Sie Ihre Mitarbeitenden über die Einführung des SchutzFuchs-Maskottchens und die damit verbundenen Belohnungs- und Motivationsmaßnahmen. Nutzen Sie interne Kommunikationskanäle wie E-Mails, Meetings und Aushänge, um das Bewusstsein zu erhöhen.
- Nutzen Sie die Gelegenheit, um Wettbewerbe und Gewinnspiele zu organisieren und das prosoziale Verhalten in Bezug auf ITS zu fördern.
- Beobachten Sie die Wirkung des Maskottchens und sammeln Sie Feedback von den Mitarbeitenden.

Die Nudges für situatives Bewusstsein (4.2) (“In-Role”-Verhalten) können ohne besondere Vorbereitungen installiert werden. Detaillierte Informationen dazu finden Sie in den stellenspezifischen Kampagnenplänen