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

Stellenspezifischer Kampagnenplan für das Ärztliche Fachpersonal

Inhaltsverzeichnis

1. Stellenspezifischer Kampagnenplan

1.1 Matching Belegschaft mit ITS-Anforderungsprofil

Dieser Kampagnenplan zielt darauf ab, ärztliches Fachpersonal auf Basis ihres Arbeitsumfangs mit direktem oder indirektem Patientenkontakt (viel vs. wenig Patientenkontakt) gezielt anzusprechen und gezielt ITS-Kompetenzen aufzubauen. Dabei werden unterschiedliche Bedrohungsvektoren für die Kompetenztestung verwendet, je nach Selbsteinschätzung der Arbeitszeit mit Patientenkontakt. Durch die Rolleneinstufung wird sichergestellt, dass die Testinhalte den individuellen Anforderungen der jeweiligen beruflichen Tätigkeit entsprechen.

Die Rolleneinstufung wird durch die folgende Frage abgedeckt: *Denken Sie bitte an einen typischen Arbeitstag. Wie viel Arbeitszeit verbringen Sie mit direktem Patientenkontakt?*

		**Rolle:** 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 Insidern) / 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.

1.2 Handlungsbedarf identifizieren mit ITS-Kompetenztests

Profil 1.1 Ärztliches Fachpersonal (behandelnd): Die Kompetenztests konzentrieren sich auf den falschen Umgang mit sensiblen Informationen, unbefugten Zugriff, die unangemessene Weitergabe sensibler Daten über ungesicherte Kommunikationskanäle und den unachtsamen Umgang mit Zugangsdaten. Diese Bedrohungsvektoren (Tabelle 1) spiegeln die hohe Verantwortung des ärztlichen Fachpersonals im Umgang mit Patienteninformationen wider.

Bezeichnung (Bedrohungsvektor)	**Beschreibung**
P 1.1.1 (Nr. 1.1)	Mitarbeitende besprichen sensible medizinische Informationen in einem öffentlich zugänglichen Raum (z.B. Stationsgang), wo unbefugte Personen die Unterhaltung mithören können.
P 1.1.2 (Nr. 1.10)	Autorisierte Mitarbeitende nutzen ihre Zugriffsrechte aus, um auf Daten zuzugreifen, die für ihre Rolle nicht bestimmt sind.
P 1.1.3 (Nr. 1.9)	Mitarbeitende teilen sensible medizinische Informationen (z. B. Patientendaten) über unsichere private Messenger-Dienste.
P 1.1.4 (Nr. 1.3)	Mitarbeitende geben Zugangsdaten unachtsam an andere Personen weiter, was potenziell zu einem unbefugten Zugriff auf das KIS führen kann.
P 1.1.5 (Nr. 1.5)	Mitarbeitende benutzen ein privates Smartphone, um Fotos von medizinischen Dokumenten oder anderen sensiblen Daten zu machen, wodurch diese Informationen in einem ungesicherten privaten Gerät gespeichert werden, das einem höheren Risiko für Datenschutzverletzungen ausgesetzt ist.

Tabelle 1: Top 5 Bedrohungsvektoren des ärztlichen Fachpersonals (behandelnd)

Profil 1.2 Ärztliches Fachpersonal (verwaltend): Hier umfassen die Testlets die Nichteinhaltung von Richtlinien für Software und Hardware, das Risiko durch Schadsoftware, die Gefahren durch gefälschte Websites, das Risiko des nicht gesperrten Bildschirms und die

Bedrohung durch Spear-Phishing und Social Engineering-Angriffe. Diese Bedrohungsvektoren (Tabelle 2) betonen die Wichtigkeit der Datensicherheit und des Schutzes interner Systeme in administrativen Rollen.

Bezeichnung (Bedrohungsvektor)	**Beschreibung**
P 1.2.1 (Nr. 1.7)	Mitarbeitende installieren ohne Genehmigung Drittanbietersoftware (z. B. Zitationsprogramme oder andere nicht zugelassene Tools) auf dem Firmenrechner, was die Sicherheit des Systems gefährden kann, da die Software nicht den internen Richtlinien oder Sicherheitsstandards entspricht.
P 1.2.2 (Nr. 1.4)	Mitarbeitende besuchen unsichere Websites, auf denen unbemerkt Schadsoftware heruntergeladen wird, die anschließend das interne Informationssystem infizieren und kompromittieren kann.
P 1.2.3 (Nr. 1.2)	Eine gefälschte Website, die einer legitimen Anbieter-Website täuschend ähnlich sieht, bringt Mitarbeitende dazu, persönliche oder vertrauliche Informationen einzugeben, die anschließend missbraucht werden können.
P 1.2.4 (Nr. 1.8)	Mitarbeitende verlassen ihren Arbeitsplatz, ohne den Bildschirm zu sperren, wodurch unbefugte Personen vorübergehend Zugriff auf sensible Informationen oder das System selbst erhalten könnten.
P 1.2.5 (Nr. 1.5)	Ein gezielter Phishing-Angriff, bei dem Mitarbeitende eine manipulierte E-Mail von einem scheinbar vertrauenswürdigen Absender erhalten und dazu verleitet werden, auf schädliche Links zu klicken.

Tabelle 2: Top 5 Bedrohungsvektoren des ärztlichen Fachpersonals (verwaltend)

1.3 Kompetenzen fördern mit ITS-Trainings

Für das Stellenprofil des ärztlichen Fachpersonals wurden sechs Trainingsvideos entwickelt, deren Inhalte und Längen in Tabelle 3 aufgeführt sind. Um das Ziel zu erreichen, frühzeitig ein breites Wissen bei Ihren Mitarbeitenden aufzubauen und die meisten Bedrohungsvektoren zeitnah anzugehen, empfehlen wir die Bereitstellung der Trainingsvideos in der in Tabelle 3 dargestellten Reihenfolge. Bitte überprüfen Sie, ob für Ihre Zertifizierungen alternative Zeiträume relevant sein könnten und berücksichtigen Sie auch saisonale Herausforderungen, wie zum Beispiel erhöhte Ausfallraten aufgrund von Krankheiten, Urlaubszeiten oder unvorhergesehenen Ereignissen, die die Teilnahme beeinträchtigen könnten.

Titel	Inhalt (Kompetenztests)	Dauer (in Minuten)
Angriffe durch Social Engineering	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, was Social Engineering ist, wie sie sich richtig im Umgang mit Social Engineering verhalten und welche weiteren Maßnahmen ergriffen werden können. (P1.2.5)	05:53
Der richtige Umgang mit Zugangsdaten	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, welche Gefahren und Konsequenzen durch einen falschen Umgang mit Zugangsdaten und unsicheren Passwörtern möglich sind, wie sie sich richtig verhalten und welche weiteren Maßnahmen ergriffen werden können. (P 1.1.4, P 1.1.2)	06:17
Umgang mit sensiblen und kritischen Informationen in sozialen Medien	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, welche Konsequenzen durch einen falschen Umgang mit sensiblen und kritischen Informationen möglich sind, wie sie sich richtig verhalten und welche weiteren Maßnahmen ergriffen werden können. (P 1.1.3, P 1.1.5)	05:31
Spoofing – Gefahr durch gefälschte Webseiten	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, was Spoofing ist und welche Gefahren durch Spoofing entstehen, wie sie sich richtig im Umgang bei dem Verdacht von Spoofing verhalten und welche weiteren Maßnahmen ergriffen werden können. (P 1.2.2, P 1.2.3)	05:35
Clean Desk – Umgang mit kritischen Informationen am Arbeitsplatz	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, welche Gefahren und Konsequenzen durch nicht-ordnungsgemäß hinterlassene Arbeitsplätze möglich sind, wie sie sich im Umgang mit kritischen Informationen am Arbeitsplatz verhalten und welche weiteren Maßnahmen ergriffen werden können. (P1.1.1, P 1.2.4)	05:22
Umgang mit Malware	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, was Malware ist, wie sie sich richtig im Umgang mit Malware-Attacken verhalten und welche weiteren Maßnahmen ergriffen werden können. (P 1.2.1)	06:37

Tabelle 3: Übersicht der Trainingsthemen für ärztliches Fachpersonal

1.4 ITS-Bewusstsein aufrechterhalten mit ITS-Nudges

Der Umgang mit sensiblen Informationen in der medizinischen Praxis stellt eine zentrale Herausforderung dar, insbesondere wenn Mitarbeitende Bilder von sensiblen Daten über private Messengerdienste an Interne oder externe Personen versenden, wie z. B. Urlaubs- oder Schichtpläne. Ein verhaltenswissenschaftlicher Ansatz zur Sensibilisierung für den verantwortungsvollen Umgang mit sensiblen Daten ist die Implementierung eines Nudges in Form von stilisierten Augenmotiven (hier: ein Fuchs). Diese visuelle Erinnerung soll das Bewusstsein der Mitarbeitenden stärken und sie dazu anregen, sensible Informationen sicher und verantwortungsbewusst zu behandeln. Die Umsetzung des Nudges erfolgt durch die Platzierung runder Sticker mit dem Fuchsmotiv an strategisch relevanten Stellen innerhalb der medizinischen Einrichtung. Diese Stellen umfassen Orte, an denen regelmäßig sensible Informationen verarbeitet oder aufbewahrt werden, wie beispielsweise Computermonitore, Aktenschränke und Bulletin Boards. Der finanzielle Aufwand für die Herstellung und Verteilung der Sticker ist mit 70 Euro für 500 Stück verhältnismäßig gering. Die eigentliche Platzierung kann schnell und effizient durch das vorhandene Personal erfolgen. Dieser Prozess erfordert keine umfangreichen Schulungen oder technische Anpassungen.

Umgang mit sensiblen Informationen in sozialen Netzwerken (Private Messengerdienste)
Problem: Versenden von Bildern von Schicht- und Urlaubsplänen an Interne oder Externe.
Lösung: Platzierung von stilisierten Augen (hier: Fuchs) an Orten mit sensiblen Informationen.
Umsetzung, Durchführung, Aufwand: Sticker, 3 cm rund; 70 €/500 St.

Tabelle 4: Sticker Schutzfuchs

Ein weiteres erhebliches Sicherheitsrisiko stellt der unsachgemäße Umgang mit sensiblen Patientendaten dar. Private Messengerdienste werden dazu genutzt, um beispielsweise schnell und unkompliziert Zweitmeinungen einzuholen. Dies geschieht außerhalb der gesicherten Krankenhausinfrastruktur und gefährdet die Vertraulichkeit und Integrität der Daten. Ein Nudge zur Sensibilisierung des ärztlichen Fachpersonals besteht in der Verteilung von Informationskarten, die strategisch auf den Schreibtischen platziert werden. Diese Karten sollen

als kontinuierliche visuelle Erinnerung dienen, die auf die Risiken der Nutzung unsicherer Kommunikationskanäle hinweisen. Die Kosten für die Produktion der Informationskarten sind mit 26 Euro für 1000 Stück sehr gering. Die Verteilung der Karten kann durch vorhandenes Personal ohne signifikanten zusätzlichen Aufwand durchgeführt werden.

Umgang mit sensiblen Informationen in sozialen Netzwerken (Private Messengerdienste)
Problem: Mitarbeitende versenden Patientendaten an Interne oder Externe über Nicht-Krankenhaus-Infrastruktur (z.B. WhatsApp) um eine Zweitmeinung einzuholen.
Lösung: Informationskarten, die auf Schreibtischen verteilt werden.
Umsetzung, Durchführung, Aufwand: Flyer, DIN A7, 400g; 26 €/1000 St. Verteilung auf Schreibtischen oder in Postfächern.

Tabelle 5: Informationskarten zum Umgang mit sensiblen Informationen in sozialen Netzwerken