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

Stellenspezifischer Kampagnenplan für das Medizinisches Fachpersonal

Inhaltsverzeichnis

1. Stellenspezifischer Kampagnenplan

1.1 Matching Belegschaft mit ITS-Anforderungsprofil

Dieser Kampagnenplan zielt darauf ab, medizinisches 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:** Medizinisches Fachpersonal	
Nr.	**Zentrale Bedrohungsvektoren**	
2.1	Einschleusen bekannter Malware in interne Informationssysteme (z.B. Viren per Mail) /Mailsystem	Der Angreifer nutzt gängige Übermittlungsmechanismen (z. B. über E-Mail), um bekannte Malware (z. B. Malware, deren Existenz bekannt ist) in Informationssysteme von Unternehmen zu installieren/einzuschleusen.
2.2	Angreifer platziert Wechselmedien mit Malware in der physischen Umgebung der Organisation (z.B. durch USB-Sticks) / USB-Laufwerk	Der Angreifer platziert Wechseldatenträger (z. B. Flash-Laufwerke), die Malware enthalten, an Orten außerhalb der physischen Grenzen des Unternehmens, an denen die Mitarbeitenden die Datenträger wahrscheinlich finden (z. B. auf Parkplätzen) und auf den Informationssystemen des Unternehmens verwenden.

2.3	Verbreiten sensibler In-formationen (z.B. durch Kommunikation über WhatsApp) / Instant-Messenger	Ein autorisierter Benutzer kontaminiert 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 ist. Die Informationen sind dem Zugriff Unbefugter ausgesetzt, so dass das Gerät, System oder Netzwerk nicht verfügbar ist, während der Schadensfall untersucht und entschärft wird.
2.4	Spear-Phishing / 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.
2.5	Social Engineering Angriffe, um Personen inner-halb der Organisation 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, Personen innerhalb von Organisationen zu überreden oder auf andere Weise dazu zu bringen, kritische/sensible Informationen (z. B. personenbezogene Daten) preiszugeben.
2.6	Falscher Umgang mit kritischen und/oder sensiblen Informationen durch autorisierte Benutzer / KIS	Ein autorisierter, privilegierter Benutzer gibt versehentlich kritische/sensible Informationen bei Nutzung des KIS/PDMS preis.
2.7	Unbefugter Zugriff auf interne Informationssysteme durch Insider (z.B Versuch Zugang zu Patientendaten zu erhalten, die normalerweise nur ärztliches Fachpersonal erhält / KIS	Ein Angreifer ist eine Person, die über eine Zugangsberechtigung zu den Informationssystemen einer Organisation verfügt, sich aber einen Zugang verschafft (oder versucht zu verschaffen), der über die Berechtigung hinausgeht.

2.8	Verbreiten sensibler Informationen (z.B. durch Posten von Bildern in sozialen Medien) / Social Media App	Ein autorisierter Benutzer kontaminiert 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 ist. Die Informationen sind dem Die Informationen sind dem Zugriff Unbefugter ausgesetzt, so dass das Gerät, System oder Netzwerk nicht verfügbar ist, während der Schadensfall untersucht und entschärft wird.
2.9	Verbreiten sensibler Informationen (mündlich) / Mitarbeitende	Ein autorisierter Benutzer kontaminiert 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 ist. Die Informationen sind dem Die Informationen sind dem Zugriff Unbefugter ausgesetzt, so dass das Gerät, System oder Netzwerk nicht verfügbar ist, während der Schadensfall untersucht und entschärft wird.
2.10	Verlust von ext. Datenträgern mit sensiblen Informationen / Mitarbeitende	Der Verlust von externen Datenträgern wie USB-Sticks, externen Festplatten oder anderen mobilen Speichermedien, die sensible Informationen enthalten, stellt einen weiteren schwerwiegenden Bedrohungsvektor dar. Wenn diese Datenträger von Mitarbeitenden verloren gehen oder gestohlen werden und diese nicht angemessen verschlüsselt sind, können Unbefugte potenziell Zugriff auf die darauf gespeicherten vertraulichen Daten erlangen.
2.11	Kein Sperren des Bildschirms bei Abwesenheit vom PC / Mitarbeitende	Wenn Mitarbeitende ihre Arbeitsplätze verlassen, ohne den Computerbildschirm zu sperren, bleibt das System ungeschützt und zugänglich für jeden, der physischen Zugang zu

		diesem Arbeitsplatz hat. Dies kann unbeabsichtigten oder bösartigen Zugriff auf sensible Informationen ermöglichen. Unautorisierte Personen könnten diese Gelegenheit nutzen, um vertrauliche Daten einzusehen, zu modifizieren oder zu entwenden, was zu Datenlecks, Datenschutzverletzungen und potenziellen rechtlichen Folgen führen kann.

1.2 Handlungsbedarf identifizieren mit ITS-Kompetenztests

Profil 2.1 Medizinisches Fachpersonal (behandelnd): Die entwickelten Testlets adressieren die physische Sicherheit von USB-Flashdrives, die Übermittlung sensibler Informationen über soziale Netzwerke, das Risiko des nicht gesperrten Bildschirms und die Gefahr durch Social Engineering. Diese Bedrohungsvektoren (Tabelle 1) reflektieren die täglichen Herausforderungen im Umgang mit Daten von Patientinnen und Patienten und der Sicherung der physischen und nicht-physischen Umgebung.

Bezeichnung (Bedrohungsvektor)	Beschreibung
P 2.1.1 (Nr. 2.2)	Mitarbeitende finden in unmittelbaren Arbeitsumgebung einen USB-Stick, auf dem sich Malware befindet.
P 2.1.2 (Nr. 2.3)	Mitarbeitende teilen sensible medizinische Informationen (z. B. Patientendaten) über unsichere private Messenger-Dienste.
P 2.1.3 (Nr. 2.8)	Mitarbeitende teilen sensible medizinische Informationen (z. B. Patientendaten) über soziale Netzwerke in der Öffentlichkeit.
P 2.1.4 (Nr. 2.11)	Mitarbeitende lassen den Stationswagen mit entsperrtem Computer unbeaufsichtigt im Stationsgang, was unbefugten Personen vorübergehenden Zugriff auf sensible Daten ermöglicht.
P 2.1.5 (Nr. 2.5)	Mitarbeitende werden von einer unbekannten Person angesprochen, die hospitieren möchte (Shoulder Surfing).

Tabelle 1 Top 5 Bedrohungsvektoren des medizinischen Fachpersonals (behandelnd)

Profil 2.2 Medizinisches Fachpersonal (verwaltend): Die Testlets beinhalten Brute-Force-Angriffe, Spear Phishing, die Einschleusung von Schadsoftware, den Verlust der Vertraulichkeit sensibler Informationen und die Bedeutung des Sperrens von Bildschirmen. Sie verdeutlichen die Bedeutung von Cybersicherheit und Datenschutz im Kontext von Pflegestations- und -bereichsleitungen (Tabelle 2).

Bezeichnung (Bedrohungsvektor)	Beschreibung
P 2.2.1 (Keine Zuordnung)	Mitarbeitende wählen ein unsicheres Passwort gewählt, welches auf persönlichen Merkmalen basiert, was das Risiko von Brute-Force-Anmeldeversuchen erhöht.

P 2.2.2 (Nr. 2.1 & 2.4)	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.
P 2.2.3 (Keine Zuordnung)	Mitarbeitende besuchen unsichere Websites, auf denen unbemerkt Schadsoftware heruntergeladen wird, die anschließend das interne Informationssystem infizieren und kompromittieren können.
P 2.2.4 (Nr. 2.10)	Mitarbeitende verlassen ihren Arbeitsplatz, ohne die physischen sensiblen Daten in einen verschließbaren Aktenschrank zu sperren, wodurch unbefugte Personen vorübergehend Zugriff auf sensible Informationen erhalten könnten.
P 2.2.5 (Nr. 2.11)	Mitarbeitende verlassen ihren Arbeitsplatz, ohne den Bildschirm zu sperren, wodurch unbefugte Personen vorübergehend Zugriff auf sensible Informationen oder das System selbst erhalten könnten.

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

1.3 Kompetenzen fördern mit ITS-Trainings

Für das Stellenprofil des medizinischen 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 3Tabelle 3: Trainingsinhalte dargestellten Reihenfolge.

Titel	**Inhalt (Kompetenztests)**	**Dauer (in Minuten)**
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. (P 2.1.4, P 2.2.4, P 2.2.5)	05:22
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. (P 2.1.5, P 2.2.2)	05:52

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. (P2.1.2, P 2.1.3)	05:59
Umgang mit Gefahren in der physischen Umgebung	In diesem Trainingsmodul lernen Ihre Mitarbeitenden, wie Attacken in der physischen Umgebung aussehen und welche Konsequenzen diese Attacken haben können, wie sie sich richtig im Umgang mit solchen Attacken verhalten und welche weiteren Maßnahmen ergriffen werden können. (P 2.2.1)	04:00
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 2.2.1)	06:23
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 2.1.1, P 2.2.3)	06:15

Tabelle 3: Trainingsinhalte

1.4 ITS-Bewusstsein aufrechterhalten mit ITS-Nudges

Die Nutzung sozialer Netzwerke durch medizinisches Fachpersonal im Krankenhauskontext stellt ein erhebliches Risiko für die Datensicherheit und die Vertraulichkeit von Patientendaten dar. Wenn Mitarbeitende Bilder teilen, die Patientendaten wie Namen, medizinische Befunde oder andere identifizierende Informationen enthalten, kann dies zu unbefugtem Zugriff auf diese Daten führen. Eine innovative Lösung zur Sensibilisierung und Verhaltensänderung besteht in der Einrichtung einer „Social Media Zone“. Dies ist ein ausgewiesener Bereich (z.B. eine Wandfläche), der speziell für das Fotografieren und Teilen von Bildern vorgesehen ist. Diese Zone hilft dabei, sicherzustellen, dass keine vertraulichen Informationen unbeabsichtigt geteilt werden. Zunächst müssen innerhalb der medizinischen Einrichtung Orte ermittelt werden, die für Social-Media-Aktivitäten genutzt werden können. Diese Bereiche sollten gut sichtbar und leicht zugänglich sein, um die Nutzung zu fördern. Die Auswahl der geeigneten

Flächen ist ein entscheidender Schritt, um sicherzustellen, dass die Social Media Zone effektiv genutzt wird. Die ausgewiesene Fläche wird optisch ansprechend gestaltet, um Mitarbeitende dazu zu ermutigen, diese Zone für ihre Social-Media-Aktivitäten zu nutzen. Dies kann durch abgesetzte Wandfarbe oder durch Klebeband erfolgen. Eine visuell attraktive Gestaltung zieht die Aufmerksamkeit auf sich und signalisiert klar, dass dies der vorgesehene Bereich für das Fotografieren und Teilen von Inhalten ist. Der Aufwand zur Einrichtung einer Social Media Zone ist überschaubar. Es erfordert die Identifizierung geeigneter Flächen, die Gestaltung und die Markierung dieser Bereiche sowie die Erstellung und Anbringung von informativen Postern. Die Kosten für Materialien wie Wandfarbe, Klebeband und Druckkosten für Poster sind gering. Die eigentliche Umsetzung kann durch das vorhandene Personal durchgeführt werden und erfordert keine signifikanten zusätzlichen Ressourcen.

Umgang mit sensiblen Informationen in sozialen Netzwerken (Social Media)
Problem: Versenden von Bildern durch Mitarbeitende, auf denen versehentlich vertrauliche Daten oder Patientinnen und Patienten zu sehen sind.
Lösung: Einrichtung einer „Social Media Zone“ (z.B. Wandfläche), die zum Fotografieren geeignet ist.
Umsetzung, Durchführung, Aufwand: Identifizierung von geeigneten Bereichen, die für Social-Media-Aktivitäten genutzt werden können. Diese Bereiche sollten attraktiv aussehen. Die Fläche wird entweder durch eine abgesetzte Wandfarbe oder durch Klebeband markiert. Das Poster informiert über den Bereich.

Tabelle 4: Social Media Zone

Ein weiteres erhebliches Sicherheitsrisiko im Krankenhauskontext ergibt sich aus dem unsachgemäßen Umgang mit sensiblen Patientendaten. Dabei werden private Messengerdienste genutzt, um schnell und unkompliziert sich über Patientenfälle auszutauschen. Diese Praxis erfolgt oft außerhalb der gesicherten Krankenhausinfrastruktur, was die Vertraulichkeit und Integrität der Patientendaten ernsthaft gefährdet. Die Gründe für die Nutzung privater Messengerdienste sind vielfältig: Die einfache Handhabung, die Vertrautheit mit den Apps und die Möglichkeit einer schnellen Kommunikation spielen eine große Rolle. Allerdings sind diese Plattformen häufig nicht für den sicheren Austausch von sensiblen Informationen ausgelegt, und die Daten könnten potenziell ungeschützt oder missbräuchlich verwendet werden.

Um das medizinische Fachpersonal für die Risiken der Nutzung unsicherer Kommunikationskanäle zu sensibilisieren wird vorgeschlagen, Poster im A3-Format Poster an den schwarzen Brettern auf den Stationen anzubringen. Bei einer Auflage von 50 Postern liegen die Kosten ungefähr bei 50 Euro, abhängig von der Druckerei und den spezifischen Anforderungen. Der finanzielle Aufwand für die Entwicklung, den Druck und die Verteilung der Poster ist somit gering. Die Erstellung und Bestellung der Poster können innerhalb von etwa einer Woche abgeschlossen werden. Die Anbringung der Poster an den schwarzen Brettern kann durch das vorhandene Personal innerhalb eines Tages erfolgen, was die Maßnahme insgesamt effizient und kostengünstig macht.

Umgang mit sensiblen Informationen in sozialen Netzwerken (Private Messengerdienste)
Problem: Versenden von sensiblen Patientendaten über unsichere private Messengerdienste.
Lösung: Poster an schwarzen Brettern. Schwarze Bretter befinden sich häufig an zentralen Punkten auf Stationen, wo sie vom medizinischen Fachpersonal regelmäßig betrachtet werden.
Umsetzung, Durchführung, Aufwand: Poster, DIN A3, auf dickem Papier (z.B. 200-300 g/m²); 50 €/50 St. Verteilung an schwarzen Brettern auf Station.

Tabelle 5: Poster - Umgang mit sensiblen Daten in sozialen Netzwerken (private Messengerdienste)