DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Umsetzungshinweise nach §75c SGB V

Arbeitshilfe Awareness

Stand: 07.12.2021

Kategorie: öffentlich

Status: Freigegeben

Version: 0.98

Kürzel: AWNS

Postfach 12 05 55
10595 Berlin
Wegelystraße 3
10623 Berlin

c/o HOPE
Avenue Marnix 30
1000 Brüssel
Telefon +32 2 540 25 50

Commerzbank AG
IBAN DE63 1004 0000 0788 4141 00
BIC COBADEFFXXX
UST-IdNr. DE119355528

www.dkgev.de

Anwendungshinweis:

Dieses Dokument sowie die vorliegenden Empfehlungen und Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt die Deutsche Krankenhausgesellschaft keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

Inhaltsverzeichnis

Aus Gründen der leichteren Lesbarkeit wird in den Beschreibungen auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten und gelten gleichermaßen für beide Geschlechter.

Dokumentenhistorie

Ver-sion	Stand	Kap,/ Seite	Beschreibung der Änderung	Bearbei-tung
0.9	24.11.21	alle	Anlage des Dokumentes	AG 75c
0.98	07.12.21	alle	Kommentierung	AG 75c

1 Einleitung

Informationssicherheit ist ein Prozess, welcher etabliert werden muss, um ein angemessenes Sicherheitsniveau herzustellen, kontinuierlich aufrechtzuerhalten und an eine sich ändernde Gefährdungs- und Bedrohungslage oder unternehmerische Veränderungen anzupassen.

Dieses Ziel lässt sich nicht allein durch technische Maßnahmen erreichen. Das liegt daran, dass sich eine Vielzahl von sicherheitsrelevanten Ereignissen und Sicherheitsvorfällen auch auf ein fehlendes Bewusstsein, unzureichende Ausbildung und/oder Sensibilisierung von Mitarbeiter*innen im Bereich der Informationssicherheit zurückführen lässt.

Um diesen Gefährdungen innerhalb eines Informationssicherheitsmanagements zu begegnen, ist es erforderlich, flankierend zu technischen Maßnahmen, auch organisatorische Maßnahmen umzusetzen. Diese bestehen insbesondere aus Regeln für den sicheren Umgang mit den eingesetzten IT-Systemen, dem verantwortungsbewussten Umgang mit Informationen und der Fähigkeit, Informationssicherheitsbedrohungen zu erkennen sowie das Wissen, wie auf das Auftreten von Informationssicherheitsvorfällen zu reagieren ist.

Eine Awareness Maßnahme muss auf die jeweilige Umgebung angepasst werden. Dabei sind die Zielgruppen (Ärzte, Pflege, Administration, usw.) und andere Aspekte zum Beispiel Digitalisierungsgrad zu berücksichtigen.

Dabei stellt Security Awareness stellt ein Zusammenspiel von

- **Wissen** „Ich weiß, was zu tun wäre“
- **Können** „In meinem Umfeld kann ich sicherheitskonform handeln“
- **Wollen** „Ich möchte sicherheitskonform handeln“

dar.

Die mit den verschiedenen Awareness-Maßnahmen verbunden Ziele sind:

- Vermindertes Risiko von Datenschutzpannen
- Vermindertes Risiko von Beeinträchtigungen der IT-Sicherheit
- Verbessertes Verständnis zum Themenkomplex Informationssicherheit
- Aufdecken von Verbesserungspotentialen in Geschäftsprozessen.

2 Sensibilisierung

Folgende Schritte und Beispiele sollen Ihnen den Anfang erleichtern:

1. Aufmerksamkeit schaffen, z. B.

   - Plakat
   - Flyer
   - Schreiben durch IS-Beauftragten oder Geschäftsleitung

2. Wissensaufbau und -ausbau sowie Schaffung von Awareness-Einstellung

   - Informationsveranstaltungen
   - Intranet-Seiten
   - E-Learnings
   - Individuelle freiwillige Beratung
   - Übungen und Planspiele

3. Verstärkung von Aufmerksamkeit, Wissen und Einstellung

   - Preise und Auszeichnungen (z. B. für richtiges Handeln)
   - Quiz und Spiele

Die wichtigste Botschaft ist: aus Fehlern müssen alle lernen. Die Frage soll nicht lauten: Wer ist schuld? Sondern was läuft beim nächsten Mal anders?

Ad hoc Sensibilisierungsmaßnahmen sind immer dann durchzuführen, wenn die aktuelle Gefährdungslage oder interne Sicherheitsvorfälle diese notwendig machen. Sie haben eine Warnfunktion und müssen möglichst schnell relevante Informationen verbreiten, um über bestimmte und konkret Gefährdungen zu informieren und Möglichkeiten zum Umgang mit der spezifischen Gefahr beinhalten. Inhaltlich liegt dabei der Fokus nicht auf der Beschreibung der Gefahr, sondern auf der Handlungsanweisung zum Umgang mit der Gefahr.

Als Medium bietet sich für diese Fälle ein gesonderter E-Mail-Verteiler an.

3 Schulung

Schulungen zur Informationssicherheit betreffen alle Mitarbeiter*innen und Führungskräfte sowie Dienstleister. Sie sind regelmäßig (mindestens zweijährlich) zu wiederholen und können je nach Größe der Organisation und der Anzahl der Schulungsteilnehmer z. B. als Präsenzveranstaltungen oder E-Learning-Kurse stattfinden. Grundsätzlich kann zwischen folgenden Schulungsmethoden unterschieden werden:

Methode	Kurzbeschreibung
E-Learning	E-Learning meint die Wissensvermittlung mittels einer elektronischen Plattform mit Grundlagenwissen ohne direkte Interaktionsmöglichkeit mit einem Referenten/Ausbilder etc. E-Learning ist sehr gut geeignet ein grundlegendes Verständnis für allgemeine Schulungsthemen aufzubauen.
Unterweisungen/Einweisungen	Unterweisungen bzw. Einweisungen meint eine komprimierte knappe Wissensvermittlung zu einem bestimmten Schulungsinhalt/Sachverhalt.
Schulungen	Schulungen sind klassische Präsenzschulungen und sind als Lehrgespräch anzulegen und durchzuführen, um die Teilnehmer zu einer aktiven Arbeit zu animieren und einen Frontalunterricht zu vermeiden. Die Teilnehmerzahl ist auf max. 20 Personen zu begrenzen und sollten insgesamt eine Länge von drei Stunden inklusive ausreichend Pausen nicht zu überschreiten. Schulungen sind frühzeitig zu planen und den Teilnehmern bekanntzugeben. Über die Teilnahme wird Protokoll geführt.
Workshop	Workshops sind Schulungen zu spezifischen Themen und/oder Problemstellungen, deren Dauer i. d. R. länger als Schulungen ausgelegt sind. Die Planung von Workshops folgt den Schulungsgrundsätzen. Workshops sollten – wenn möglich – außerhalb der regulären Arbeitssituation durchgeführt werden.
Aus- und Weiterbildungen	Aus- und Weiterbildungen sind grundsätzlich lehrgangsgebunden durch qualifizierte Bildungseinrichtungen durchzuführen.

Folgende Schritte stellen die Basis für ein umfassendes Schulungskonzept dar:

- Schulungsbedarf ermitteln
- Zeitplan für Schulungsmaßnahmen definieren
- Schulung und Sensibilisierung der Führungskräfte und Mitarbeiter

Mögliche Inhalte von Schulungsmaßnahmen sind:

- Informationssicherheitsmanagement
- Umgang mit Passwörtern
- Sicherheit und E-Mail
- Phishing
- Malware
- Mobiles Arbeiten
- Physische Sicherheit
- Umgang mit Sicherheitsvorfällen
- Verhalten im Notfall
- Datensicherung
- Dokumentation und Informationssicherheit

- Umgang mit personenbezogenen Daten (Datenschutz)

Neben der Ermittlung der Schulungsthemen sind insbesondere auch die unterschiedlichen Perspektiven der einzelnen Zielgruppen bei der Gestaltung der Schulungs- und Sensibilisierungsinhalte zu berücksichtigen. Dies bezieht sich einerseits auf die Positionen (z. B. Führungskräfte) der Mitarbeiter*innen und andererseits auf das Tätigkeitsfeld (medizinisch/pflegerische Tätigkeit, Verwaltungstätigkeit, IT-Administration usw.).

Lernziele sind integraler Bestandteil jeder Schulungsplanung, da sie einerseits Anforderungen an die inhaltliche Gestaltung der Wissensvermittlung stellen und andererseits die Auswahl der Schulungsmethodik bedingen.

Lernziel	Kurzbeschreibung
Kennen	Das Lernziel **Kennen** ist das niedrigste Lernziel. Dieses Lernziel meint, dass den Mitarbeitern*innen ein Schulungsinhalt/Sachverhalt zur Kenntnis gebracht wird. Es kann nicht erwartet werden, dass der/die Mitarbeiter*innen den zur Kenntnis gebrachten Schulungsinhalt/Sachverhalt selbständig wiedergeben und erklären kann,
Verstehen	Das Lernziel **Verstehen** bedeutet eine Aufbereitung von Schulungsinhalten/Sachverhalten derart, dass bei den Mitarbeitern*innen ein grundlegendes Verständnis für die Informationssicherheit ausgebildet wird. Die Mitarbeiter*innen sind in der Lage, das Erlernte insbesondere Grundregeln zum sicheren Umgang mit Informationswerten umzusetzen.
Anwenden	Das Lernziel **Anwenden** bedeutet eine Aufbereitung von Schulungsinhalten/Sachverhalten derart, dass bei den Mitarbeitern*innen ein tiefergehendes Verständnis für die Informationssicherheit aufgebaut wird, sodass sie in der Lage sind, das Erlernte mit eigenen Worten erklären und es selbständig – auch als Transferleistung – umsetzen zu können.

4 Übungen

Regelmäßige Übungen stellen die beste Methode dar, um die Lernziele aus Schulungen effizient zu vertiefen und die Inhalte bei den Teilnehmenden zu festigen, aber auch um Abläufe zu proben bzw. trainieren

Hier eine Auswahl von Übungsszenarien:

- Testen von IT-Notfällen (einzelne Geräte, Gesamt- bzw. Teil-Netz, einzelne bzw. viele IT-Dienste, Ransomware/unbrauchbare Dateien)
- Testen von Wiederherstellungsplänen (Einspielung von Backups, Neu-Installation von IT-Systemen, z. B. Clients für die Verwaltung oder Visite oder für Server und Dienste)
- E-Mail- bzw. Phishing-Kampagnen um an Information (Namen, Passwörter) zu kommen oder Fehlverhalten zu provozieren.
- Planspiel zum Ausfall eines Kernsystems (z.B. Labor)

Über den Schulungsaspekt hinaus kann mit Übungen die Notfallvorsorge auch Dritten gegenüber nachgewiesen werden.