AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

www.aok-verlag.info/ds-im-blick

Ausgabe Nov/Dez 2023 | **Seite 1**

Inhalt

Social Engineering 2.0

Das Thema Social Engineering ist auch im Umfeld von Gesundheitseinrichtungen eine Gefahr, die betrachtet und bewertet werden muss. Darauf aufbauend sollten Gesundheitseinrichtungen Maßnahmen planen, um das Risiko von Social Engineering-Attacken zu minimieren. Eine gute Schulungsstrategie und spezielle Awarenessmaßnahmen scheinen insofern unumgänglich.

Sven Venzke-Caprarese

Social Engineering als elementare Gefährdung

Wie wichtig es ist, dass sich Gesundheitseinrichtungen mit dem Thema Social Engineering beschäftigen, zeigt ein Blick auf die „elementaren Gefährdungen“ des Bundesamts für Sicherheit in der Informationstechnik (BSI). So zählt das BSI 47 elementare Gefährdungen auf, wozu neben Gefährdungen wie beispielsweise Feuer, Wasser, Ausfall von Versorgungsnetzen, unbefugtes Eindringen in Räumlichkeiten und IT-Systeme auch eine eigene Gefährdungskategorie für „Social Engineering“ gehört.

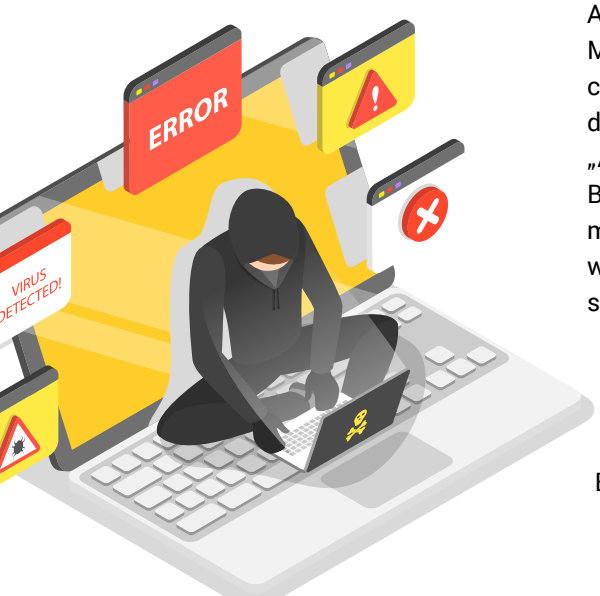
Insbesondere Einrichtungen, die ein Informationsmanagement nach

ISO 27001 auf der Basis von IT-Grundschutz aufbauen wollen, müssen sich also um diese Gefährdung kümmern und sie angemessen behandeln. Aber auch im Rahmen anderer Informationssicherheitsmanagementansätze darf das Thema nicht zu kurz kommen.

Was ist Social Engineering?

Das BSI verweist darauf, dass es beim Thema Social Engineering um die Ausnutzung des Faktors Mensch geht und dass Social Engineering genutzt wird, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Das BSI weist auch darauf hin, dass hierbei häufig menschliche Eigenschaften ausgenutzt werden, wie etwa Hilfsbereitschaft, Vertrauen, Angst oder Respekt.

Bei einem Social Engineering-Angriff werden also Menschen manipuliert, damit der Angreifer die Organisation schädigen kann. Hierbei kommen (je nach der erhofften Beute) teilweise sehr ausgefeilte Tricks zum Einsatz.



Beispiele für Social Engineering Attacken

Phishing

Die wohl bekannteste und am häufigsten auftretende Variante des Social Engineerings sind die sogenannten Phishing-Mails. Hier werden E-Mails versendet, die aufgrund von gefälschten Absenderadressen oder E-Mail-Inhalten den Empfänger dazu bewegen sollen, eine bestimmte Handlung vorzunehmen z. B.

- eine Anlage zu öffnen, die Schadcode enthält,
- einen Link anzuklicken, der Schadcode nachlädt,
- in die Kommunikation einzusteigen und Informationen preiszugeben oder Vertrauen aufzubauen,
- Nutzernamen und Passwörter in gefälschte Anmeldemasken einzugeben,
- etc.

Der Phantasie des Angreifers sind hier kaum Grenzen gesetzt. Zum Glück können sich Organisationen vor einigen Angriffsvarianten im Vorfeld mit Hilfe von Virenscannern, Firewalls, Spam-Filtern etc. gut schützen.

Am Ende schützen alleine diese Maßnahmen aber nicht ausreichend. Denn tatsächlich muss für diese Angriffe immer wieder eine „Awareness“ geschafft werden. Die Beschäftigten müssen also regelmäßig geschult und sensibilisiert werden. Hierzu kann neben spezifischen Schulungen auch das Durchführen von Phishing-Kampagnen gehören. Bei solchen simuliert die Organisation einen breiten Phishing-Angriff und sendet an die Beschäftigten simulierte „Phishing-Mails“. Danach wird meist ausgewertet, wie viele Beschäftigte auf eine solche E-Mail hereingefallen wären und dann mit weiteren Maßnahmen reagiert.

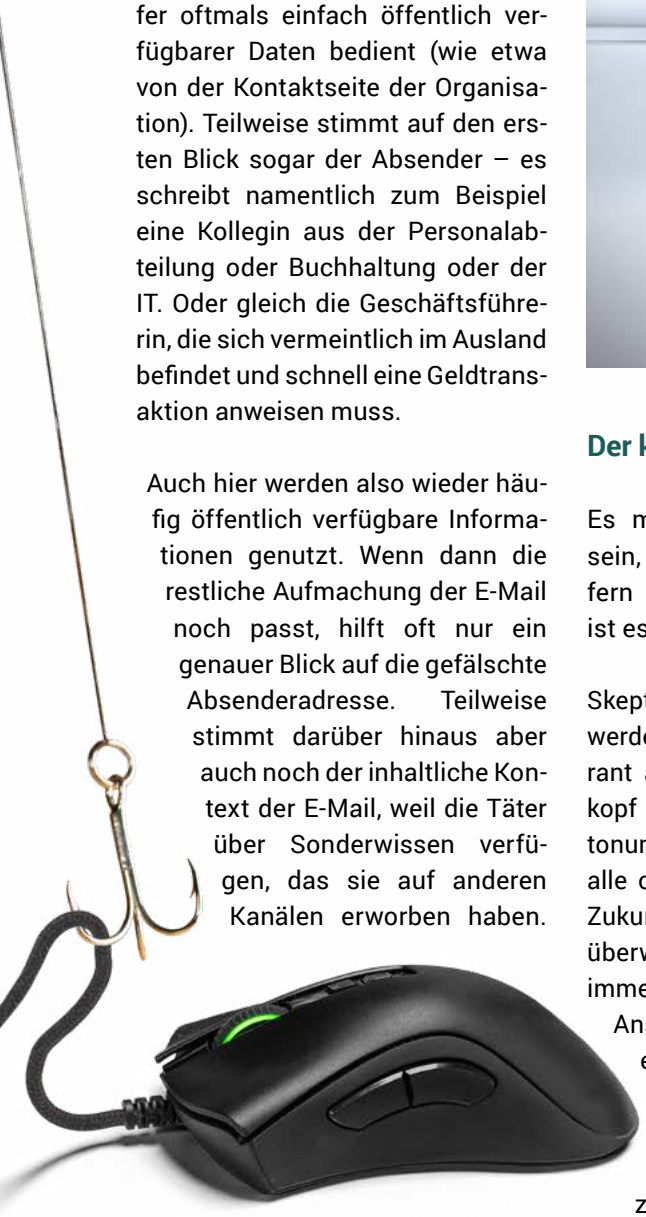
Auch datenschutzrechtlich ist das Durchführen von Phishing-Kampagnen übrigens ein Thema – denn die Verarbeitung der Auswertungen muss datenschutzrechtlich betrachtet werden. Zudem kann im Vorfeld eine Information nach Art. 13 DSGVO erforderlich werden. Diese ist keineswegs kontraproduktiv, sondern kann zum Beispiel auch einige Wochen vor der Kampagne erfolgen. Dann erhöht sie für eine Zeit sogar die Aufmerksamkeit der Beschäftigten. Sofern eine Phishing-Kampagne geplant wird und die Gesundheitseinrichtung über eine Mitarbeitervertretung verfügt, muss außerdem geprüft werden, wie diese zu beteiligen ist.

Die meisten Phishing-Mails werden in der Praxis automatisch erzeugt. Selbst dann sind sie zwar gut gemacht, aber doch sehr oft an verschiedenen Kriterien zu erkennen, wie etwa

- Rechtschreib- und Satzbaufehler,
- unpersönliche Anreden,
- merkwürdige Absenderadressen, die teilweise auch nicht mit dem vermeintlichen Namen übereinstimmen,
- merkwürdige Versanddomains (also der Teil nach dem @),
- Aufforderung, auf Links zu klicken oder Anhänge zu öffnen,
- im Inhalt geht es um Geld oder Überweisungen,
- etc.

Teilweise sind die Phishing-Mails aber auch aufwändiger erstellt. So ist es keine Seltenheit mehr, dass Phishing-Mails eine korrekte persönliche Anrede enthalten und der Empfänger namentlich begrüßt wird. Hier haben sich die Angreifer oftmals einfach öffentlich verfügbarer Daten bedient (wie etwa von der Kontaktseite der Organisation). Teilweise stimmt auf den ersten Blick sogar der Absender – es schreibt namentlich zum Beispiel eine Kollegin aus der Personalabteilung oder Buchhaltung oder der IT. Oder gleich die Geschäftsführerin, die sich vermeintlich im Ausland befindet und schnell eine Geldtransaktion anweisen muss.

Auch hier werden also wieder häufig öffentlich verfügbare Informationen genutzt. Wenn dann die restliche Aufmachung der E-Mail noch passt, hilft oft nur ein genauer Blick auf die gefälschte Absenderadresse. Teilweise stimmt darüber hinaus aber auch noch der inhaltliche Kontext der E-Mail, weil die Täter über Sonderwissen verfügen, das sie auf anderen Kanälen erworben haben.



Hier wird also mit viel Aufwand ganz gezielt „gephisht“ und nicht einfach das „Netz ausgeworfen“. Dieses Vorgehen nennt man dann Spear-Phishing.

Der klassische Brief

Es muss nicht immer die E-Mail sein, die als Köder von den Angreifern ausgeworfen wird. Manchmal ist es auch der gute alte Brief.

Skeptisch sollte man zum Beispiel werden, wenn der langjährige Lieferant auf vermeintlich echtem Briefkopf mitteilt, man habe seine Kontonummer gewechselt und auch alle offenen Rechnungen mögen in Zukunft nur noch auf das neue Konto überwiesen werden. Hier sollte immer eine Rückfrage bei bekannten Ansprechpartnern des Lieferanten erfolgen, ob dies seine Richtigkeit hat.

Organisationen, die vor kurzem eine Marke beim Deutschen Patent- und Markenamt angemeldet haben, sollten Rechnungen dieses Amtes, die per Brief eingehen, besonders skeptisch gegenüberstehen. Denn die Marken werden vor dem Eintrag veröffentlicht, damit Gegenrechte geltend gemacht werden können. Jeder sieht also, wer wann welche Marke angemeldet hat und kann diese Informationen nutzen, um eine falsche Rechnung zu übersenden.

Auch hier sind der Phantasie keine Grenzen gesetzt. Wie ist es eigentlich mit der Aufforderung eines Patienten per Brief, die Organisation möge doch bitte eine Kopie aller personenbezogenen Daten übersenden – und weil man umgezogen sei, bitte an die neue Anschrift, die noch nicht im System ist. Hier benötigt jede Organisation einen klaren Prozess bis hin zur Identitätsprüfung und eine Sensibilisierung der Beschäftigten, Auskunftsersuchen einerseits nicht unter den Tisch fallen zu lassen und andererseits nicht in vorauseilendem Gehorsam Daten an unbefugte Personen herauszugeben. Im Zweifel muss also nach der Übersendung einer (teilgeschwärzten) Personalausweiskopie gefragt werden. Obwohl diese Form der Identitätsprüfung in der Praxis weit verbreitet und wohl auch akzeptiert ist, kann man mit etwas krimineller Energie und Grafikprogrammkenntnissen eigentlich auch diese Hürde leicht überwinden. Eine wirkliche Lösung scheint sich hier noch nicht etabliert zu haben.

Das Telefonat – mit Anrufmaschine

Social Engineering macht aber nicht nur vor E-Mail und Briefversand halt. Auch am Telefon kann versucht werden, Menschen zu manipulieren. Angreifer verwenden hierzu sogar teilweise Anrufmaschinen. So ruft zum Beispiel „Europol“ an und spielt eine Bandansage ab, man sei Opfer eines Kreditkartenbetrugs geworden und wenn man die „1“ drückt, würde man zu einem „hilfsbereiten Beamten“ weitergeleitet. Tatsächlich landet man jedoch direkt in den Fängen der Betrüger, die dann noch schnell die Kreditkartendaten nebst Sicherheits- und Pincode abfragen.

Das Telefonat – mit erarbeiteter Legende

Gewiefter ist es hingegen, wenn Angreifer versuchen, sich als IT-Mitarbeitende auszugeben und von Beschäftigten am Telefon versuchen, eine Fernwartungssitzung freigeben zu lassen. Dabei können Angreifer ggf. sogar auf viel Sonderwissen zugreifen, das sie sich im Vorfeld beschafft haben.

So könnte folgender Fall auftreten: Ein Angreifer beschafft sich die Informationen, wer in der Organisation Administrator in der IT-Abteilung ist über die im Internet veröffentlichten Kontaktdaten der Organisation – z. B. Paul Müller. Er ruft dann einen beliebigen Beschäftigten der Organisation an und behauptet, Paul Müller sei krank und man müsse jetzt ein großes Update durchführen. Der Beschäftigte wird skeptisch und antwortet, das große Update sei von der IT doch erst für nächste Woche Dienstag angekündigt und außerdem habe er doch heute mit Paul Müller gesprochen. Für den Angreifer also ein Fehlschlag.

Wirklich? Nein, denn eigentlich wäre dieser Versuch ein voller Erfolg gewesen. Denn der Angreifer hätte so die Information bekommen, dass und wann das nächste große Update geplant ist. Mit diesen Informationen könnte nun bei einem weiteren Beschäftigten ein neuer Versuch gestartet werden. Diesmal könnte man sich als neuer Kollege von Paul Müller ausgeben, der das für nächste Woche angekündigte große Update schon einmal per Fernwartungszugang vorbereiten wolle und man müsse nur die Supportseite des Dienstleisters

im Internet öffnen, die Remotesitzung freigeben. Man kann sich nun fragen, wie viele Beschäftigte auf diesen Trick, ggf. noch angereichert um weitere Informationen, hereinfallen würden. Vermutlich die wenigsten. Das gefährliche ist jedoch, dass es schon ausreicht, wenn auch nur ein Beschäftigter auf den Trick hereinfällt.

Beschäftigte sollten daher auch für solche Szenarien sensibilisiert und vorbereitet werden. Und wenn man merkt, dass man gerade einen Angriff abgewehrt hat, also nicht auf den Anruf hereingefallen ist, sollte man wissen, an wen man sich in der Organisation wendet, damit ggf. alle Beschäftigten darüber informiert werden können, dass derzeit Angriffsversuche per Telefon durchgeführt werden.

Das Telefonat – und der Einsatz künstlicher Intelligenz

Vermutlich noch nicht groß in der Praxis verbreitet, aber durchaus denkbar ist auch das folgende Szenario: Die Leitung der Organisation ruft in der Buchhaltung an und möchte eine Zahlung anweisen. Die Beschäftigten dort sind normalerweise extrem skeptisch. Schon in der Vergangenheit gab es ähnliche Versuche aber diese wurden nicht wirklich ernst genommen, da jedes Mal sofort erkannt wurde, dass es sich nicht um die Stimme der Leitungskraft handelte.

Dieses Mal ist die Stimme aber eindeutig die der Leitungskraft und ein kurzer Dialog mit Rückfragen, die nur ein Beschäftigter der Organisation wissen kann (z. B.: wer ist Administrator und wann ist das nächste Update geplant) wurden richtig beantwortet und die Zahlung angewiesen. Die Leitungskraft bestreitet am nächsten Tag aber überhaupt angerufen zu haben.

Wie kann so etwas möglich sein? Wirklich schwer wäre dies in der heutigen Zeit tatsächlich nicht mehr. Hat die Leitungskraft zum Beispiel in der Vergangenheit ein aufgezeichnetes Interview gegeben, bei einem Podcast mitgemacht oder auf dem YouTube Channel der Einrichtung einen Beitrag gebracht? Dann können Angreifer die dort vorhandenen Stimmdaten nutzen, um mit Hilfe eines Programms, das auf künstlicher Intelligenz beruht, die Stimme zu imitieren. Sogenannte Sprachwechseltools könnten dann in der Lage sein, die Stimme des Angreifers in nahezu Echtzeit in die Stimme der Leitungskraft zu verwandeln.

Fazit

Schulung und Awareness im Hinblick auf die elementare Gefährdung des Social Engineerings sollten in jeder Einrichtung zur Selbstverständlichkeit werden.

Dabei sollte neben dem üblichen Angriffsszenario (Phishing) unbedingt darauf hingewiesen werden, dass es durchaus auch andere Angriffsvektoren gibt.

Querschnittsprüfung an Evangelischen Krankenhäusern

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland (BfD EKD) führt aktuell eine Querschnittsprüfung an Evangelischen Krankenhäusern durch, um den aktuellen Stand zur Einhaltung der datenschutzrechtlichen Vorgaben zu erheben. In über 60 Fragen geht es im Schwerpunkt um die Verarbeitung und den Schutz von Patientendaten. Große inhaltliche Überraschungen waren nicht zu erwarten und gibt es auch nicht. Dennoch lohnt sich eine Auseinandersetzung, um, exemplarisch am BfD EKD, die Schwerpunktsetzung der Aufsichtsbehörden im Gesundheitssektor zu erkennen.

Dr. Sebastian Ertel

Dokumentationen

Ein erster großer Baustein der Querschnittsprüfung betrifft die Dokumentation. So sind insbesondere folgende Dokumente vorzulegen:

Rechte-Rollenkonzept des KIS

Liste der Dienstleister
Die verantwortliche Stelle ist aufgefordert, eine Liste der Dienstleister vorzulegen, mit denen Verträge zur Auftragsverarbeitung geschlossen wurden.

Behandlungsvertrag mit Datenschutzinformationen
Hierdurch wird geprüft, inwieweit die Transparenzpflichten gegenüber den Betroffenen erfüllt und ob Einwilligungen in Verträgen versteckt eingebunden werden.

Formulare zur Einholung von Einwilligungen

Datenschutzrechtliche Einwilligungen müssen hohe Hürden überwinden. Neben der Informiertheit werden hier vor allem die Widerrufbarkeit und die Folgen eines Widerrufes im Fokus der Betrachtung stehen.

Verzeichnis über Verarbeitungstätigkeiten (VVT)
Jede Verarbeitung personenbezogener Daten muss im VVT ausführlich dokumentiert sein. Das VVT dient hier zudem der Verifizierung der Liste der Dienstleister. Auftragsverarbeiter müssen in beiden Dokumenten aufgeführt werden, sodass Deltas schnell identifiziert werden können.

Löschkonzept
Das Löschkonzept muss einerseits aufzeigen, welche Aufbewahrungspflichten bzgl. der verschiedenen Datenkategorien bestehen und wie deren Löschung nach Fristablauf umgesetzt wird.

Umsetzung der OH KIS

Ein weiterer wesentlicher Prüfungspunkt betrifft die Umsetzung der Orientierungshilfe Krankenhaus-Informationssysteme (OH KIS). Dieses in der 2. Auflage (2014) bestehende Dokument definiert die Rechtsauffassung der Aufsichtsbehörden im Zusammenhang mit der Verarbeitung von Patientendaten im Krankenhaus-Informationssystem.

Werden für Vertretungen oder Bereitschaftsdienste zusätzliche Berechtigungen nur temporär zugewiesen (Frage 38)?

Diese Frage zielt darauf, dass ein Zugriff auf die Daten eines Patienten nur den Mitarbeitenden der Ärzteschaft, Pflege und Verwaltung möglich sein darf, die in die Bearbeitung des konkreten Falles eingebunden sind. Alle anderen Mitarbeitenden der Einrichtung dürfen keinen Zugriff auf die Daten nehmen. Nur in Ausnahmefällen (Notfälle, Arzt vom Dienst) darf ein Zugriff erfolgen, unter erneuter Eingabe des individuellen Passwortes. In diesem Zusammenhang ist es zudem wichtig, dass die außerordentlichen Zugriffe protokolliert und diese Protokolle regelmäßig ausgewertet werden. Die Umsetzung des Prozesses wird in der Querschnittsprüfung ebenfalls abgefragt Fragen 42 und 43).

Gibt es Vorkehrungen, die Daten von eigenen Mitarbeitenden, die als Patienten aufgenommen werden, in besonderer Weise zu schützen oder zu anonymisieren? (Frage 44)

Die Frage ist verwirrend, soweit diese auf eine Anonymisierung von Daten abzielt. Durch die Anonymisierung geht jegliche Zuordnung der Daten zu einer natürlichen Person verloren. Gerade im Hinblick auf die Dokumentationspflichten medizinischer und pflegerischer Maßnahmen und die gesetzlichen Aufbewahrungspflichten muss die Frage richtigerweise auf eine Pseudonymisierung, bei der eine Zuordnung zur betroffenen Person mit entsprechendem Zusatzwissen hergestellt werden kann, gerichtet sein.

Auch diese Frage zielt auf die OH KIS ab. Mitarbeitende, die sich bei ihrem Arbeitgeber in medizinische Behandlung begeben, müssen darauf vertrauen dürfen, dass deren Daten vor Zugriffen der Kollegen besonders geschützt werden. Der Schaden, der für die Betroffenen bei unberechtigter Kenntnisnahme entsteht, ist noch mal höher als bei klassischen Patienten.

Daher sind diese Datensätze besonders zu schützen. Die Krankenhaus-Informationssysteme bieten hier verschiedene Funktionalitäten an. Einerseits können entsprechende Datensätze so markiert werden, dass diese ohne entsprechende Berechtigungen nicht im KIS aufgefunden werden können. Andererseits besteht die Möglichkeit, diese Datensätze von Anfang an zu versiegeln. Jeder Aufruf bedeutet einen protokollierten Siegelbruch, der bei der notwendigen Kontrolle der Protokolldaten sofort festgestellt wird.

Werden immer personenspezifische Nutzerkonten verwendet oder gibt es auch sogenannte Gruppen-Accounts? (Frage 37)

Gruppen-Accounts werden von mehreren Nutzern verwendet und bergen daher die Gefahr, dass beispielsweise Verletzungen der Vertraulichkeit, Verfügbarkeit und Integrität von Daten keinem Täter zugeordnet und damit keine erforderlichen Abhilfemaßnahmen getroffen werden können. Dabei ist grundsätzlich zwischen Client-Ebene und den verschiedenen Spezialanwendungen zu unterscheiden. Gerade auf Client-Ebene können Gruppen-Accounts sinnvoll sein, damit sich die Mitarbeitenden nicht permanent an- und abmelden müssen. Das ist jedoch nur solange zulässig, wenn auf der Client-Ebene keine individuellen Datenverarbeitungen der einzelnen Mitarbeitenden erfolgen und die auf dieser Ebene zugänglichen Dateien und Dokumente für alle Kontoinhaber relevant sind und keinen Personenbezug haben. Zudem muss der Zugriff auf Spezialsoftware (KIS, RIS; LIS, PACS, diagnostische Anwendungen) anschließend mit einer personenspezifischen Anmeldung unter Eingabe eines individuellen Passwortes erfolgen. Eine Anmeldung per Single Sign-on, bei dem sich der Nutzer nur einmalig unter Verwendung des Authentifizierungsverfahrens authentisieren muss, ist bei Gruppen-Accounts nicht geeignet, weil mit der Anmeldung auf Client-Ebenen automatisch alle Anmeldungen bei den Spezialsoftwaren einhergehen

Etablierte Prozesse

Ein weiterer Punkt betrifft das Organisatorische, insbesondere, inwieweit bestimmte Handlungen in Prozessen abgebildet sind.

Das betrifft beispielsweise die Vergabe, Änderung und den Entzug von Berechtigungen zu Spezialanwendungen.

Aber auch der Umgang mit Protokolldaten, vor allem die Auswertungen und revisionssichere Vorhaltung, werden erfragt.

Kurznotiz

Immer wieder: Datenpannen durch offene Verteiler

Ein Klassiker unter den Datenpannen ist der Versand von E-Mails an einen großen Adressatenkreis, ohne Nutzung der BCC-Funktion des E-Mail-Programmes. BCC steht für „blind carbon copy“. Was bewirkt BCC? Die in das BCC-Feld eingetragenen Empfänger erhalten die E-Mail ganz normal, jedoch wird ihre E-Mail Adresse den anderen Empfängern nicht angezeigt. Dadurch wird verhindert, dass alle Adressaten einer Mail sehen, wer ebenfalls Adressat dieser Mail ist.

Wird die BCC-Funktion nicht genutzt und stattdessen in „CC“ versendet, stellt dies regelmäßig eine Datenpanne dar. Findet diese auch noch im Gesundheitssektor statt, ist diese meldepflichtig, kann Informationspflichten gegenüber den betroffenen Personen auslösen und ein Bußgeld nach sich ziehen.

Das passierte Anfang Januar 2023 beispielsweise im Universitätskrankenhaus Padua (Italien). Ein Krankenhausmitarbeitender hatte eine E-Mail versandt. In dieser bat er um die Einwilligung zur Teilnahme an einer klinischen Studie mit dem Schwerpunkt „Herzchirurgische Eingriffe“. Dabei hatte er sämtliche Empfänger in das CC-Feld eingefügt, wodurch alle Patientinnen und Patienten des Krankenhauses bekannt wurden, die auf eine Herztransplantation warteten.

Die italienische Aufsichtsbehörde hat in diesem Fall ein Bußgeld i.H.v. 5000 € verhängt, was im konkreten Fall noch sehr wenig anmutet. Tatsächlich wären darüber hinaus sogar Schadensersatzansprüche der betroffenen Patienten denkbar.

Quelle: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9861356

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-0 | Fax 02642 931-215
Mail: fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen
Geschäftsführung: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese
Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden.
Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: GettyImages, AOK-Verlag

Wir bemühen uns um eine geschlechtergerechte Sprache. Weil wir Ihnen den Lesefluss so angenehm wie möglich gestalten möchten, wählen wir in vielen Fällen dennoch die männliche Form. Die Inhalte beziehen sich aber immer auf alle Geschlechter. Wenn nicht, weisen wir ausdrücklich darauf hin.

Praxishandbuch für Datenschutzbeauftragte im Gesundheitswesen

Welche Patientendaten dürfen an wen und in welcher Form übermittelt werden? Wie ist ein Empfangsbereich im Krankenhaus zu strukturieren, damit die Privatsphäre jedes Einzelnen gewährleistet wird? Wie muss ein Datenschutzkonzept aussehen, damit es als Grundlage für einen Audit dienen kann? Und wer hat eigentlich auf welche Patientendaten Zugriff?

Die Herausforderung ist, dass die innerbetrieblichen Abläufe durch die Umsetzung datenschutzrechtlicher Vorgaben nicht beeinträchtigt werden sollen - ein Spagat, der gemeistert werden muss. Hinzu kommt, dass viele Datenschutzbeauftragte diese Tätigkeit neben ihrem Hauptaufgabengebiet ausüben und sich ein fundiertes Wissen im IT-Bereich erst aneignen müssen, um mit Kollegen oder Externen auf Augenhöhe zu kommunizieren.

Das Handbuch „Datenschutz im Gesundheitswesen“ greift die typischen Arbeits- und Problemfelder auf und liefert Lösungen, die Rechtssicherheit, Nachhaltigkeit und Akzeptanz bei Aufsichtsbehörden bieten. Der Schwerpunkt des Handbuches liegt in der praktischen Umsetzung der datenschutzrechtlichen Vorgaben im betrieblichen Alltag, bspw. bei den spezifischen Anforderungen in den verschiedenen Bereichen des Gesundheitswesens, wie Krankenhaus oder Arztpraxis.

Im exklusiven Online-Kundenbereich finden Sie das Werk als E-Book. Mittels PDF-Download laden Sie kapitelweise Ihr Handbuch herunter und können es direkt an Ihrem Rechner einsetzen. So sind Sie unabhängig von Ihrem Arbeitsort und haben jederzeit Zugriff auf die Datenschutzbestimmungen.

- 2 Ordner mit Register im Format DIN A5,
- ca. 1.500 Seiten Inhalt
- ISBN: 978-3-553-43000-5
- Preis **195,00 €** inkl. MwSt.
- Uneingeschränkter Online-Zugriff
  inkl. 3-4 kostenpflichtige Nachtragslieferungen
  pro Jahr zum Preis von jeweils **89,90 €** inkl. MwSt.
  und versandkostenfreier Zusendung im Inland.

HIER bestellen