Christoph Hönicke beantwortet wichtige Fragen zur IT-Sicherheitsrichtlinie nach §75b SGB V der Kassenärztlichen Bundesvereinigung

IT-Sicherheit: Eine UTM (Einheitliches Gefahren-Management) -Hardware-Firewall ist nicht die Lösung aller Probleme

Die Digitalisierung hat auch vor dem Gesundheitswesen nicht halt gemacht und fordert von den Praxis-Inhaberinnen und -Inhabern viel ab. Mit der digitalen Kommunikation und dem Datenaustausch im Gesundheitswesen sind natürlich auch die Anforderungen an die Datensicherheit gewachsen und werden auch in Zukunft ein wichtiges Thema sein, mit dem sich jeder Praxisinhaber beschäftigen muss. Für viele ist das ein Thema, dem sie allerdings am liebsten aus dem Weg gehen würden. Ich spreche heute mit einem von der KBV-zertifizierten IT-Dienstleister, der jeden Tag in verschiedensten Praxen unterwegs ist, der genau weiß, was den Praxis-Inhaberinnen und -Inhabern abverlangt wird und der die Probleme in der Umsetzung der IT-Sicherheitsrichtlinie der KBV genauestens kennt.

Schnelle Frage zum Einstieg:
Was macht die IT-Sicherheit aus Ihrer Sicht so wichtig?
Die Cyberangriffe auf Medatixx in Eltville, MediaMarkt/ Saturn oder auch das Bürgerbüro in Ludwigslust-Parchim sind alles Zeichen dafür, dass die Cyberkriminalität vor unserer Haustür und leider auch Praxistür steht. Genau aus diesem Grund hat die KBV im Januar 2021 eine Richtline zur IT-Sicherheit auf den Weg gebracht (§75b SGBV). Mit dem Ziel einen Standard festzulegen, den jede Praxis als Handreiche nehmen kann, um die eigene Praxis-IT abzusichern. Dabei handelt es sich um einen Mindeststandard, der aber bereits eine gute Absicherung schafft.

Die Sicherheitsrichtlinie der KBV ist für den Laien an manchen Stellen möglicherweise überfordernd. Können Sie sie in einfachen Worten zusammenfassen und uns einen kleinen Einblick geben, was für welche Praxis relevant ist?
Der interessante Teil der IT-Sicherheitsrichtlinie für Praxis-Inhaberinnen und -Inhabern sind sicherlich die Anlagen, denn dort werden die Anforderungen definiert, die die Praxen erfüllen müssen. Die Anforderungen wachsen, je größer eine Praxis ist, daher werden die Praxen nach Größen eingeteilt. Zusätzlich werden medizinische Großgeräte und die Komponenten der Telematik in weiteren Anlagen benannt.

Aber woher weiß ich, welche Anforderungen ich in meiner Praxis umsetzen muss?
Die allermeisten Praxen zählen zu den kleineren Praxen und müssen daher Anlage 1 (Eine Praxis ist eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen) und Anlage 5 (Anforderungen für Dezentrale Komponenten der Telematik Infrastruktur) umsetzen – für diese beiden Anlagen sind das 41 Punkte.

Ist es aus Ihrer Sicht möglich, dass Praxisinhaber das allein bewältigen können?
Die Anforderungen sind schon jetzt sehr komplex und sie werden auch in Zukunft eher zunehmen als weniger werden. Da ich davon ausgehe, dass Praxis-Inhaberinnen und -Inhaber Experten ihres Faches sind, aber eben weniger Expertise in technischen Fragen haben, empfehle ich das Hinzuziehen eines zertifizierten IT-Dienstleisters. Zur Umsetzung

der Richtline werden und wurden von der KBV IT-Technik-Firmen zertifiziert, diese kann man in einer Liste der KBV sichten.

Es gibt auf dem Markt so viele Angebote von IT-Dienstleistern. Woher weiß ich, welches das Richtige für meine Praxis ist?
Die Anforderungen in der Sicherheitsrichtlinie bieten in der Umsetzung leider sehr viel Spielraum zur Auslegung. Das führt dazu, dass es eine Flut von Angeboten auf dem Markt gibt, die kaum zu überblicken ist. An dieser Stelle spreche ich nicht als IT-Dienstleister, sondern möchte Sie bitten folgende Punkte zu berücksichtigen:

1. IT-Dienstleister
   Haben Sie einen eigenen IT-Dienstleister, dem Sie vertrauen? Fragen Sie ihn, welches Konzept er hat bzw. mit wem er zusammenarbeitet. Wichtig ist aus meiner Sicht auch, ob der Dienstleister von der KBV zertifiziert ist, denn das Zertifizierungsverfahren ist sehr komplex und anspruchsvoll und bietet somit viel Sicherheit für die Praxen.
2. Vergleichen Sie das Angebot immer mit den Punkten in den entsprechenden Anlagen. Werden in dem Angebot alle Punkte der Richtlinie erfüllt und umgesetzt?
3. Vergleichen Sie das Angebot auch mit anderen Angeboten auf dem Markt.
4. Fragen Sie Kolleginnen und Kollegen

Als IT-Laien fällt es vielen Praxis-Inhaberinnen und -Inhabern schwer, Angebote zu vergleichen und das Richtige herauszufiltern. Haben Sie da aktuell Beispiele, worauf man achten kann?
Ich kann sehr gut nachvollziehen, dass es sehr schwierig ist, Angebote herauszufiltern, die alle geforderten Punkte auch wirklich abdecken. Und ja, es gibt tatsächlich auf dem Markt sehr viele Angebot die den Inhalt der Richtline nicht korrekt wiedergeben. Angefangen von UTM Firewalls, die als verpflichtend verkauft werden bis hin zu Dienstleistern, die WLAN als verboten hinstellen. Diese Punkte finde ich nicht in den Anlagen.

Ein Beispiel: In Anlage 1 Punkt 32 wird gefordert, dass Netzübergangspunkte abgesichert werden sollen. Auch das Wort Hardware-Firewall wird benutzt. Dazu gibt es viele Angebote, die eine UTM-Hardware-Firewall als die Lösung aller Probleme darstellen. Aber an dieser Stelle vielleicht mal eine kurze Erklärung, dass eine Hardware Firewall nicht eine UTM für 1500€ plus Installation und plus Wartung bedeutet. Eine Hardware-Firewall kann auch ein Produkt für 300 € sein. Wir reden dort auch nur von einem Punkt der Anlage 1. Verstehen sie mich nicht falsch, ich möchte dass die Praxen so sicher wie nur möglich sind. Aber ich möchte nicht, dass den Praxis-Inhaberinnen und -Inhabern Dinge als Pflicht oder Zwang verkauft werden, die auch anders gelöst werden können.

Zudem herrscht in vielen Praxen Verunsicherung oder auch manchmal die Überzeugung darüber, dass die Anschlussart des Konnektors seriell bzw. in Reihe für eine ausreichende Absicherung der Praxen sorgt und sie keine Firewall benötigen. Generell findet man das in der KBV-Richtlinie, aber der Konnektor ist keine Firewall und man hat kaum Möglichkeiten etwas einzustellen. Die Erfahrung hat gezeigt, dass bestimmte Funktionen, wie das Update des Virusscanners oder die Fernwartung nicht funktionieren und auch nicht vom IT-Betreuer freigeschaltet werden können. Ein Konnektor in Reihe kann also eine Übergangslösung sein, aber für eine vernünftige und störungsfreie Umsetzung der Richtline sollte lieber Technik eingesetzt werden, die auch als Firewall hergestellt wurde.

Oder noch ein anderes Beispiel: Auch der Punkt 33, der Netzwerkplan wird von vielen IT'lern weggelächelt. Gerade diesen Punkt halte ich als Nachweis aber für sehr wichtig.

Oder die Anforderung einer TLS –Verbindung (automatische Transportverschlüsselung) im Praxisverwaltungssystem, die seit 01.01.2021 verpflichtend ist, wurde in den meisten Systemen erst zum 01.09.2021 umgesetzt und ist immer noch nicht in allen Systemen möglich.

Was ist aus Ihrer Sicht noch wichtig für die gute Umsetzung der IT-Sicherheit in der Praxis?
Oftmals vergessen wir, dass die Technik nicht die einzige, ich nenne es jetzt mal uncharmant, „Fehlerquelle" in der IT-Sicherheit ist. Auch das Praxispersonal hat keine IT-Ausbildung und muss viel Neues lernen. Allein mit DSGVO, §75b und der Digitalisierung im Allgemeinen müssen die Angestellten in einer Praxis viel umsetzen, was sie in Ihrer Ausbildung im besten Fall angerissen haben. Ich kann also auch den Praxen hier wieder nur raten, sensibilisieren sie Ihr Personal! Von vielen IT-Firmen werden Schulungen angeboten, die erklären, wie man sich im Notfall verhalten muss, was man beachten muss, was passiert, wenn man das nicht beachtet. Diese Schulungen sind laut DSGVO und QM sowieso verpflichtend.

Dazu noch ein Beispiel aus der Praxis: Ich stelle in den Praxen immer ein, dass der Browserverlauf und die Cookies nach dem Schließen der Anwendung gelöscht und keine eingespeicherten Passwörter mehr zugelassen werden. Diese Passwort-Speicherung ist die größte Diskussion in jeder Praxis: Von „Wie soll ich mir das alles merken?" bis hin zu „So kann man doch nicht arbeiten." Wenn ich dann aber vorführe, wie schnell man an alle eingespeicherten Passwörter gelangen kann und wie einfach ich diese abschreiben kann, wird vielen Praxen und auch dem Praxispersonal klar welche Sicherheitslücke dies beinhaltet.

Das sind nur ein paar Beispiele aus der Praxis, die die Umsetzung für Praxis-Inhaberinnen und -Inhabern erschweren und die aus meiner Sicht, ein eigenständiges Umsetzen der Richtline durch den Praxisinhaber oder das Praxispersonal unmöglich machen. Mir ist sehr bewusst, dass Praxis-Inhaberinnen und -Inhabern keine IT'ler sind und die Aussage der KBV „die Ärzte können das alleine" nicht wirklich stimmen kann.

Herr Hoenicke ist Geschäftsführer der Hoenicke Systembetreuung GmbH.
Das Interview wurde geführt von Claudia Wollbrück, selbstständige IT-Praxisberaterin

12.11.2021

Zertifizierte Berater zur IT-Sicherheitsrichtlinie und viele weitere Informationen finden Sie auf der Internetseite der Kassenärztlichen Bundesvereinigung
https://www.kbv.de/media/sp/KBV_ISAP_Dienstleister_ZERT_P75b_SGBV.pdf und
https://hub.kbv.de/site/its