



Motivierte Cyberschutzarbeit – Cyberschutz-Beauftragte

Cyberschutzarbeit ist für viele Mitarbeiter ein leidiges Übel oder wird sogar als „Nervfaktor“ betrachtet. Wo sowieso schon wenig Zeit für die Versorgung der Patienten vorhanden ist, werden Belehrungen und Erklärungen zur Bedeutung des Cyberschutzes schnell lästig. Dass der Praxis-Cyberschutz und deren Einhaltung vor allem auch durch das Datenschutzgesetz (DSGVO) und der kommenden IT-Richtlinie (KBV und BSI) geregelt sind, ist zwar unumstritten – doch ohne die motivierte Mitarbeit des Praxispersonals kaum in die Realität umzusetzen. Dabei ist der Frustrfaktor bei den Datenschutzkräften hoch, denn ohne die notwendige Verständigung der Cyberschutz-Zusammenhänge verpuffen viele Bemühungen.

Doch wie lassen sich Lösungen um die tägliche Cyberarbeit als motivierte Teamarbeit vermitteln? Ob sich Mitarbeiter nur mit Vernunft und rationalen Argumenten davon überzeugen lassen, sich an Verfahrensanweisungen zu halten, sei dahingestellt. Aus psychologischer Sicht wird dies jedenfalls bezweifelt, da sich viel emotionales Konfliktpotenzial im Bereich Datenschutz und Qualitätsmanagement abzeichnet.

Neben der emotionalen Ebene spielt auch die individuelle Persönlichkeit jedes einzelnen Teammitglieds eine entscheidende Rolle. Die Frage lautet deshalb kurzum: Wie können positive emotionale Aktivierungen ausgelöst werden, um einem „Faulpelz“ Tatendrang und einer „Spaßbremse“ Humor zu vermitteln?

Gravierende Mängel in der Realität

Großer Zeitmangel in der Praxis, damit verbundener Stress, nicht genügend qualifiziertes Personal und mangelnde Schulungen führen häufig zu einem vernachlässigten Daten- und Cyberschutz. Diese sind allerdings von elementarer Bedeutung.

Auch bei den externen IT-Unternehmen oder auch eigenen Datenschutzbeauftragten konnte in acht von zehn Fällen Mängel erkannt werden. Datensicherungen und deren Funktion werden häufig nicht überprüft und dementsprechend auch nicht an geforderten BSI-Standards angepasst. Ein Leistungsverzeichnis ist zwar Pflicht, aber dennoch nicht immer sinnvoll, beispielsweise wenn das Zeitmanagement nicht übereinstimmt. Praxis-Datenschutzbeauftragte haben neben ihrer Aufgaben im Bereich Datenschutz oftmals noch drei oder vier weitere Aufgaben in der Praxis.

Diese Daten sind Ergebnisse, die im Rahmen des *Heidelberger Datenschutz-Ratings* (siehe Infokasten) erfasst wurden. Weiteren Erkenntnissen des Datenschutz-Rankings zufolge entsprachen technische und organisatorische Maßnahmen (TOM) bzw. Notfallpläne nicht den Erfordernissen der Praxis und waren nicht an die Einrichtung angepasst. In einigen Räumlichkeiten lagen Datensicherungen und Patientendaten auf den Tischen und Stühlen, Passwörter klebten unter der Tastatur. Ebenso waren Behandlungsräume nur durch dünne Wände bzw. Vorhänge getrennt.

Heidelberger Cyberschutz-Ranking

Die Initiative Heidelberger Datenschutz-Rating wurde durch Praxismanagement Bublitz-Peters (Heidelberg) gemeinsam mit Mitarbeitern aus Behörden, Kliniken und Arztpraxen entwickelt. Auf einer deutschlandweiten Datenschutzkarte (www.datenschutz-zertifizierung.de) können dabei geprüfte Einrichtungen im Gesundheitswesen gefunden werden. Es wird nach den DSGVO und BSI-Grundlagen, PBP-Richtlinie und nach PBP-Checkliste bzw. einem Selbstauskunftsbogen der Behörden geprüft und regelmäßig aktualisiert.

Auszug der Mängelliste des Heidelberger Cyberschutz-Ratings:

CYBERSCHUTZ

- Keine Cyberschutzschulung
- Kein Cyberschutz-Notfallkoffer
- Keine Cyberschutz-Notfallschulung
- Keine ausreichende IT-Sicherheit
- Keine Cyberschutz-Versicherung

DATENSCHUTZ

- DSGVO-Umsetzung nicht ausreichend
- TOMs nicht umgesetzt
- Dienstleister nicht in die Verantwortung genommen (Bsp. Konnektor)
- Datenschutzbeauftragte nicht richtig weitergebildet bzw. nicht unabhängig
- Externer Datenschutzbeauftragter nicht ausreichend spezialisiert (BSI-Cyberschutz)

UNTERWEISUNGSPFLICHT

- Nicht/nur teilweise vorhandene Unterweisungsnachweise

Instrumente motivierter Cyberschutzarbeit/Cyberschutz-Koordinator

Um nun die herrschenden Cyberschutzmängel zielgerichtet zu beseitigen, ist wie eingangs beschrieben die Motivation des Personals unerlässlich. Dabei kommt es vor allem darauf an, das Verantwortungsbewusstsein der einzelnen Mitarbeiter zu wecken.

Die gezielte Kenntniserweiterung der Datenschutzbeauftragten durch regelmäßige praxisnahe Schulungen ist dabei jedoch ebenso wichtig.

Coaching

Das Ziel der Cyberschutzbeauftragten ist es, erfolgreich die für die Praxis erarbeiteten Qualitätsmerkmale umsetzen zu können. Dabei kann sie die Mitarbeiter durch emotionale Stärkung in das gemeinsame Boot holen.

Grundstein hierfür bildet wie so häufig ein respektvoller Umgang untereinander, um Bloßstellung und Demotivierung zu vermeiden. Zudem wird der Übermittlung sinnvoller Cyberschutzaufgaben eine große Bedeutung beigemessen: Aktive Beteiligung der Mitarbeiter ist der Schlüssel zu motivierter Cyberschutzarbeit. Dem gegenüber steht die passive Informationsaufnahme.

Ein weiterer Punkt stellt die Motivation durch Humor dar. Dabei können kleine „Schmankerl“ behilflich sein („Datenschutz-Flop der Woche“ oder Ähnliches). Die positive Assoziation, die dabei mit dem Thema Cyberschutz entsteht, wirkt sich ebenso positiv auf die Motivation aus.

Gleichzeitig sollten Unaufmerksamkeiten in den Mitarbeitern schlussendlich eine milde Art des Schamgefühls erzeugen, damit die Behebung derselben die naheliegendste Option darstellt.

Was Heidelberger Cyberschutz-Coaching bietet

Virtuelle Schulungen

Auch Online-Schulungen für die Datenschutzbeauftragte sind zu empfehlen. Dabei werden schwerpunktmäßig verschiedene Themengebiete behandelt, so beispielsweise Cyberqualität, IT-Sicherheit, Datenschutz oder Qualitätsmanagement. Es wird an relevanten Stellen auf Videos oder Dokumente (Standards) zugegriffen, die gelesen werden müssen und nicht übersprungen werden können. Ein weiterer Vorteil ist die ortsunabhängige und eigenständige Arbeit vor dem PC.

Virtuelle Schulungen fördern neben den Fachkompetenzen auch Schlüsselkompetenzen wie Projektmanagement, Mitarbeiterführung und Zeitmanagement. Von Persönlichkeitsstärkung (Frustrationstoleranz, Konfliktfähigkeit, Empathie) über Vortrags- und Präsentationstechniken bis hin zu Gruppenanalyse, Streitgespräch und Teambuilding – diese Fähigkeiten fügen sich am Ende zu einem kompetenten Gesamtbild zusammen, von welchem die komplette Praxis profitiert.

Fazit

Cyberschutzarbeit ist Teamarbeit! Datenschutzbeauftragte müssen ihre Kollegen dort abholen, wo sie stehen. Der Trainer muss die Talente seiner Mitspieler kennen und wissen, wie er sie fördert bzw. fordert. Positive Emotionen sowie das Gefühl der Selbstwirksamkeit spielen eine wichtige Rolle für die Motivation und jegliche Form des Lernens – ein Lächeln sagt mehr als tausend Worte, ein Lob bringt mehr als tausend Anweisungen. Einmal nachfragen, wie es im Urlaub war, hilft oft schon über Alltagsfrust hinweg.

Interessante Links

- www.cyberschutzzertifizierung.de
- www.datenschutzzertifizierung.de

Kontakt

MARK PETERS

Praxismanagement Bublitz-Peters GmbH & Co. KG
Rohrbacher Straße 28 | 69115 Heidelberg

Telefon: +49 (62 21) 43 85 00

E-Mail: info@bublitz-peters.de | www.bublitzpeters.de

