Abwehr von Cyberattacken in der ambulanten und stationären Gesundheitsversorgung durch regelmäßige Mitarbeiterschulungen

Im Gesundheitswesen ist es von besonderer Bedeutung, dass Mitarbeiter regelmäßig geschult werden, um das Risiko von Cyberattacken zu minimieren und im Falle eines Angriffs erfolgreich abzuwehren.

Bedrohungslage steigt kontinuierlich

Die Gesundheitsbranche ist ein lukratives Ziel für Cyberkriminelle, da sensible Patientendaten wie medizinische Aufzeichnungen und Finanzdaten leicht verkauft oder missbraucht werden können.

Der Schaden durch Cyberattacken im Gesundheitswesen kann erheblich sein und zu einem wochenlangen Stillstand der Praxis- oder Klinik-IT führen. Aufgrund der Sensibilität der verarbeiteten Daten im Gesundheitssystem wird von Gesundheitsunternehmen wie Praxen und Kliniken ein besonders hohes Schutz- und Sicherheitsniveau erwartet und in den Datenschutzverordnungen (z.B. DSGVO) festgeschrieben.

Die Verletzung von Datenschutzmaßnahmen im Gesundheitswesen sowie erfolgreiche Cyberattacken auf Gesundheitsdaten bedeuten nicht nur einen erheblichen Reputationsverlust für betroffene Einrichtungen, sondern können auch empfindliche Strafen nach sich ziehen, wenn ein Fehlverhalten der Einrichtung, z.B. durch mangelhafte Datenschutzmaßnahmen, nachgewiesen werden kann.

Bedrohungen (er-)kennen und vermeiden

Mitarbeiterschulungen sind ein wichtiger Teil einer umfassenden Strategie zur Verteidigung gegen Cyberangriffe im Gesundheitswesen. Durch Schulungen können Mitarbeiter über die neuesten Bedrohungen informiert werden und lernen, wie sie sich selbst und das eigene Unternehmen schützen können.

Beispielsweise können sie lernen, wie sie Phishing-Angriffe erkennen und vermeiden können, indem sie auf bestimmte Merkmale manipulierter E-Mails achten, wie z.B. eine ungewöhnliche Absenderadresse oder eine fordernde Tonart.

Unerwartet oder unaufgefordert mitgesendete Anhänge in veralteten Dateiformaten (z.B. Word-Dateien mit *.doc statt *docx) oder Links auf unbekannte Webseiten sollten ebenfalls misstrauisch machen. Sie können manipuliert sein und Trojaner oder Ransomware auf dem eigenen Computer installieren und diese im IT-Netzwerk der Einrichtung verbreiten.

Absender manipulierter Mails können sowohl unbekannte als auch vermeintlich bekannte Personen sein. Bei Verdacht auf Manipulation von E-Mails sollten Mitarbeiter sich über andere Kanäle wie z.B. das Telefon absichern, bevor sie Anhänge öffnen oder auf Links klicken.

Wichtige Cybersecurity-Maßnahmen im Gesundheitswesen

Im Gesundheitswesen ist es von besonderer Bedeutung, dass umfassende Maßnahmen zur Verteidigung gegen Cyberangriffe eingehalten werden. Einige haben wir hier für Sie zusammengestellt:

1. **Regelmäßige Schulungen der Mitarbeiter**
   Mitarbeiter sollten regelmäßig über die neuesten Bedrohungen und Maßnahmen zur Verteidigung gegen Cyberangriffe geschult werden. Nur mit diesem Wissen ist es möglich, Angriffe von Hackern zu erkennen und abzuwehren.
2. **Verwendung sicherer Passwörter**
   Alle Mitarbeiter sollten starke, einzigartige Passwörter verwenden und diese regelmäßig ändern,

um einen Zugriff durch Unbefugte zu verhindern. Voreingestellte Passwörter (z.B. an Routern) sollten unmittelbar nach Inbetriebnahme neuer Geräte geändert werden.

3. **2-Faktor-Authentifizierung nutzen**
   Viele Webseiten (z.B. Banken) und Cloudsysteme (z.B. Office 365) bieten die 2-Faktor-Authentifizierung als weitere Sicherheitsmaßnahme an. Nutzen Sie diese Möglichkeit, bei der Ihr Zugriff z.B. durch den Versand eines Codes per SMS oder durch eine Authentifizierungs-App zusätzlich verifiziert wird. Das nervt manchmal, bietet aber besonderen Schutz.
4. **E-Mail Check**
   Drei Kurze Fragen, die Sie sich bei jeder Mail stellen sollten.
   - Kommt Ihnen der Absender bekannt vor?
   - Ist der Betreff sinnvoll?
   - Ist der mitgeschickte Anhang oder Link erwartet?

   Falls Sie sich unsicher sind, ob Sie der Mail vertrauen können, kann ein kurzer Anruf beim Absender meist schon Abhilfe leisten.
5. **Nutzung der Bildschirmsperre**
   Schalten Sie beim Verlassen Ihres Computers immer die Bildschirmsperre ein. Gerade dann, wenn in der Umgebung Publikumsverkehr herrscht und Dritte einen Blick auf dem Bildschirm werfen könnten. Dies geht besonders leicht mit den folgenden Tastenkombinationen:
   Windows + **L** (Windows) oder **Command** + **Control** + **Q** (Mac)
6. **Vermeidung unsicherer Netzwerke**
   Mitarbeiter sollten davon absehen, mit mobilen Endgeräten und Notebooks über öffentliche oder unsichere Netzwerke auf sensible Daten oder Systeme zuzugreifen.
7. **Regelmäßige Überprüfung und Aktualisierung von Sicherheitssystemen**
   Es ist wichtig, dass alle Systeme regelmäßig auf Sicherheitslücken überprüft werden, um sicherzustellen, dass sie gegen Angriffe geschützt sind. Deshalb immer aktuelle Updates einspielen und die Antivirensoftware sowie die Firewall aktuell halten.
8. **Einsatz von Verschlüsselungstechnologie**
   Sensible Daten sollten mit einer geeigneten Verschlüsselungstechnologie geschützt werden, um sicherzustellen, dass sie im Falle eines Datenverlusts oder einer Datenpanne unlesbar bleiben.
9. **Regelmäßige Backups**
   Es ist wichtig, dass regelmäßige Backups aller sensiblen Daten erstellt werden, um sicherzustellen, dass diese im Falle eines Angriffs oder einer Datenpanne wiederhergestellt werden können. Backups sollten an unterschiedlichen Orten aufbewahrt werden.
10. **Überwachung von Netzwerken und Systemen**
    Es ist wichtig, dass Netzwerke und Systeme überwacht werden, um potenzielle Angriffe frühzeitig zu erkennen und zu verhindern.

Dies sind nur einige Maßnahmen, die im Gesundheitswesen eingehalten werden sollten, um sicherzustellen, dass sensible Patientendaten und das eigene EDV-Netzwerk geschützt sind.

Aufgrund der immer neuen Angriffswege und -techniken ist nicht nur das Maßnahmenbündel ständig an die aktuelle Bedrohungslage anzupassen, sondern Mitarbeiter regelmäßig für diese neuen Gefahren durch Schulungen zu sensibilisieren. Dabei bieten sich insbesondere digitale Fortbildungen an, da sie rasch aktualisiert und leicht und kostengünstig an alle Mitarbeiter ausgeliefert werden können.

Schulungen zur Informationssicherheit: Jeder einzelne Mitarbeiter zählt

Durch die regelmäßige Schulung aller Mitarbeiter wird sichergestellt, dass jeder die neuesten Bedrohungen und Maßnahmen zur Abwehr gegen Cyberangriffe kennt.

Die schwächsten Glieder in der Kette sind bei Cyberattacken der uninformierte Mitarbeiter sowie veraltete Hard- und Software.

Von besonderer Bedeutung sind regelmäßige Awareness-Schulungen in der ambulanten Gesundheitsversorgung, z.B. in Arztpraxen, ambulanten Pflegediensten und bei Heilmittelerbringern. Durch die dezentrale Organisation und die Eigenverantwortung jedes einzelnen Praxis- bzw. Einrichtungsbetreibers bestehen hier sehr unterschiedliche IT-Installationen. In Ermangelung umfangreicher IT-Erfahrungen sind hier häufiger Sicherheitsrisiken anzutreffen als in größeren Einheiten, Krankenhäusern und Unternehmen mit eigener IT-Abteilung. Häufige Schwachstelle in Praxen ist z.B. veraltete Hard- und Software. Diese Lücken werden von Cyberkriminellen systematisch und häufig automatisiert ausgenutzt und können zu massiven Schäden in den betroffenen Einrichtungen führen.

Darüber hinaus kann eine regelmäßige Schulung der Mitarbeiter dazu beitragen, dass sich ein besseres Bewusstsein für die Bedeutung von Cybersicherheit im Gesundheitswesen entwickelt. Dies soll dazu führen, dass Mitarbeiter ihre Verantwortung für den Schutz von Patientendaten ernster nehmen und sich bewusster verhalten, wenn sie mit solchen Daten arbeiten.

KBV-Sicherheitsrichtlinie

Für Arztpraxen hat die Kassenärztliche Vereinigung Sicherheitsempfehlungen herausgegeben, deren Einhaltung ein flächendeckendes Sicherheitsniveau in Praxen und MVZ garantieren soll. Maßnahmen werden differenziert für kleine, mittlere und große Praxen aufgeführt. Sie gliedern sich nach strukturellen Maßnahmen und Verhaltensempfehlungen für den Arbeitsalltag und sollten allen Mitarbeitern regelmäßig vermittelt werden.

Die KBV-Sicherheitsrichtlinie bietet viele wertvolle Tipps und Hinweise, die auch in anderen Gesundheitseinrichtungen sinnvoll eingesetzt werden können.

Wissen und Sensibilisierung schützen

Mitarbeiter im Gesundheitswesen sollten regelmäßig geschult werden, um Cyberangriffe erfolgreich abzuwehren. Durch die sich ständig ändernde Bedrohungslage und neue Angriffsmethoden genügt es nicht, eine einmalige Schulung anzubieten.

Die meduplus GmbH Berlin hat in Zusammenarbeit mit IT-Sicherheitsexperten spezielle Onlinekurse zur Cybersecurity sowie zum Datenschutz in Gesundheitseinrichtungen entwickelt. Diese können einzeln oder im Paket mit einem interaktiven Datenschutz-Ordner für das gesamte Praxisteam gebucht werden. Der Ordner enthält zusätzliche Checklisten und Musterformulare und kann auch für die Dokumentation regelmäßiger Teamschulungen genutzt werden.

Verbandsmitglieder erhalten Nachlässe von 20% auf die Angebote der meduplus GmbH.

Mit den kontinuierlich aktualisierten digitalen Fortbildungen zu IT-Sicherheit und Cybersecurity können Inhaber von Praxen und Gesundheitseinrichtungen sicherstellen, daß alle Mitarbeiter kontinuierlich über die aktuellen Angriffsmethoden und Cybergefahren informiert sind und Strategien zu deren Vermeidung kennen sowie im Arbeitsalltag umsetzen.

Dr. Jörg Ansorg
Geschäftsführer meduplus GmbH Berlin