Presseinformation

Sicherheit von Gesundheitsdaten auf dem Prüfstand

Daten sind aus unserer Welt nicht mehr wegzudenken. Wie aber steht es um die Sicherheit der Daten von österreichischen Patient*innen – also den Schutz vor Verlust, Zerstörung und Missbrauch? Mittels einer Befragung und eines White-Hat-Hack-Experimentes sind die Österreichische Plattform Patientensicherheit und das KFV dieser Frage auf den Grund gegangen. Trotz des generell hohen Datensicherheitsniveaus konnten dabei häufig vorkommende Schwachstellen identifiziert werden. Höhere Passwortsicherheit, regelmäßige Backups und Softwareupdates könnten in Verbindung mit der Sensibilisierung Mitarbeitender maßgeblich zur Optimierung der Datensicherheit im Gesundheitssektor beitragen.

Wien, 30. März 2022. Die COVID-19 Pandemie hat Gesundheitsdienstleister in aller Welt mit unvorhersehbaren Belastungen konfrontiert und die Menge an Gesundheitsdaten nicht nur vervielfacht, sondern auch in den Mittelpunkt des allgemeinen Interesses gerückt. Kriminelle witterten darin die Chance auf lukrative Geschäfte. So stellte die Internationale Kriminalpolizeiliche Organisation (INTERPOL) seit Beginn der Pandemie eine deutliche Zunahme der Ransomware-Attacken auf Krankenhäuser und andere Gesundheitsdienstleister fest. „Die Gefahr von Cyber-Angriffen zieht auch an Österreichs Gesundheitseinrichtungen nicht spurlos vorüber. Gerade in diesem hochsensiblen Bereich muss alles getan werden, um die Sicherheit der Daten und somit der Patientinnen und Patienten zu gewährleisten“, ist **Dr. Maria Kletečka-Pulker, Geschäftsführerin der Österreichischen Plattform Patientensicherheit**, überzeugt. Denn von Cyberangriffen betroffene Gesundheitsdienstleister zahlen mitunter einen hohen Preis: Sie werden nicht nur finanziell geschädigt, sondern auch an ihrer medizinischen und pflegerischen Arbeit gehindert.

Datensicherheit auf dem Prüfstand

Die Plattform Patientensicherheit und das KFV sind der Frage auf den Grund gegangen, wie es um die Sicherheit von Gesundheitsdaten in Österreich aktuell steht. Das Ergebnis der umfassenden Analyse bestehend aus Expert*inneninterviews, Befragung und White-Hat-Hack ergibt, dass die Sicherheit von Patient*innen-Daten in Österreich bereits auf einem erfreulich hohen Niveau rangiert. Im Zuge einer auf Selbstselektion basierenden Befragung unter Gesundheitsdienstleistern gaben 7 Prozent der Befragten an, im letzten Jahr tatsächlich einen Cyberangriff erlebt zu haben – in allen Fällen konnte der Angriff durch bestehende Sicherheitsmaßnahmen abgewehrt werden. Jedoch wurden im Zuge der Befragung auch potenzielle Schwachstellen offengelegt: So nutzt mehr als die Hälfte (52%) der Befragten Endgeräte am Arbeitsplatz auch für private Zwecke, die überwiegende Mehrheit der Befragten verwendet zudem nur eine einfache Passwortabfrage (63%), um die Endgeräte vor Fremdzugriffen zu schützen. Bei mehr als zwei Drittel aller befragten Dienstleister (69%) kommen idente Passwörter auf mehr als einem Gerät zum Einsatz. „An Geräten, die zu Verarbeitung sensibler

Daten genutzt werden, sollte private Nutzung die Ausnahme, die Zwei-Faktor-Authentisierung hingegen Standard sein – sie ist eine ebenso einfache wie effektive Möglichkeit zur Erhöhung der Datensicherheit“, so **Dr. Armin Kaltenegger, Leiter des Bereiches Eigentumsschutz im KFV.** Sinnvoll ist auch der Einsatz eines Systems unterschiedlicher Berechtigungsstufen für Mitarbeitende, so dass jede Person nur die Zugriffsrechte hat, die sie unbedingt benötigt. Auf diese Weise wird das Risiko, dass ungeschultes Personal mit Datensätzen hantiert, die für die Arbeit nicht notwendig sind, minimiert.

Gesundheitsrisiko Datenverfügbarkeit

Während zumindest zwei Drittel der Befragten regelmäßige Updates (69%) und Spamschutz (66%) einsetzen, sieht es bei anderen Schutzmaßnahmen schon spärlicher aus: Nicht einmal jeder zweite befragte Gesundheitsdienstleister (48%) führt regelmäßig externe Datenbackups durch. Diese sind jedoch essenziell, um im Falle eines Ransomware-Angriffs den Betrieb aufrecht zu erhalten. „Sowohl in der Diagnostik als auch bei der Behandlung spielen computergestützte Systeme heutzutage eine tragende Rolle. Wenn medizinisches Personal Maßnahmen einleiten muss und dazu Informationen über den Zustand einer zu behandelnden Person benötigt, kann jede Verzögerung oder Unterbrechung gesundheitliche Konsequenzen nach sich ziehen“, gibt **Anna Teufel, Leiterin der Geschäftsstelle der Österreichischen Plattform Patientensicherheit**, zu bedenken. Vor allem im niedergelassenen Gesundheitsbereich ist das Schutzniveau noch ausbaufähig. „In der Regel verfügen nur große Dienstleister über Protokolle für den Umgang mit Störfällen oder Cyberattacken. Ein solches Protokoll kann jedoch im Falle eines Angriffs die interne Reaktionszeit und den entstandenen Schaden auf ein Minimum reduzieren“, so **Kaltenegger.** IT-Dienstleister wiederum sind gefordert Lösungen zu entwickeln, die auch für kleine Dienstleister leist- und anwendbar sind.

Datensicherheit und der Faktor Mensch

Im Rahmen eines sogenannten White-Hat-Hacks wurden die Informationssysteme eines Gesundheitsdienstleisters mit dessen Einverständnis einem gezielten IT-Sicherheitstest unterzogen: Fehlende Softwareupdates, die Verwendung von Standardpasswörtern und mangelhaft geschützte Administratorenrechte waren nur einige der Schwachstellen, die dabei offengelegt wurden. „Besonders deutlich wurde dabei, welche wesentliche Rolle der Faktor Mensch im Bereich der Datensicherheit spielt, denn: Im Praxistest führte das aufmerksame Verhalten der Mitarbeitenden in mehreren Fällen zum Misslingen der Angriffe“, so **Kaltenegger**. Wenn es um Fragen der IT-Sicherheit geht, sind gut geschulte und sensibilisierte Mitarbeitende mindestens genauso wichtig wie die Absicherung der technischen Infrastruktur. Das gilt für alle Unternehmen – ganz besonders jedoch für den Gesundheitsbereich, wo die Arbeitsbelastung oft überdurchschnittlich hoch und die Daten ganz besonders schützenswert sind.

Bildmaterial
Pressefotos stehen Ihnen unter dem folgenden Link zum Download zur Verfügung:
https://www.apa-fotoservice.at/galerie/28164
Abdruck honorarfrei. Bildnachweis: © KFV/APA-Fotoservice/Juhasz

Rückfragehinweis:
Pressestelle KFV (Kuratorium für Verkehrssicherheit)
Tel.: 05-77077-1 919 I E-Mail: pr@kfv.at I www.kfv.at