Thieme

Cybersicherheit in Arztpraxen und Krankenhäusern

Viele Arztpraxen und Krankenhäuser in Deutschland sind unzureichend vor Hackerangriffen geschützt. Dabei können die Folgen verheerend sein: Cyberkriminelle können mit gestohlenen Patientendaten Lösegeld erpressen oder medizinische Geräte wie Infusionspumpen gezielt manipulieren. Umfragen zeigen, dass viele Ärzte die Bedrohung durch Cyberkriminalität unterschätzen.

Die wohl bekannteste Cyberattacke auf eine medizinische Einrichtung in Deutschland ereignete sich im Jahr 2016. Hacker versperrten Mitarbeitern des Lukaskrankenhauses in Neuss den Zugang zu allen digitalen Daten, um Lösegeld zu erpressen. Das Krankenhaus war tagelang nur eingeschränkt arbeitsfähig, und obwohl das Haus den Lösegeldforderungen nicht nachkam, entstand ein Schaden von etwa 1 Million Euro. Was nach Krimi klingt, ist kein Einzelfall: Eine Umfrage der Unternehmensberatung Roland Berger aus dem Jahr 2017 hat gezeigt, dass von bundesweit 500 befragten Krankenhäusern 2 Drittel schon einmal einem Hackerangriff zum Opfer gefallen sind. Im Sommer 2019 sind gerade erst mehrere Einrichtungen des Deutschen Roten Kreuzes von Cyberkriminellen angegriffen worden.

Niedergelassene Ärzte unterschätzen Risiko

Wie ein Branchenreport des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) ergeben hat, denkt jeder zweite niedergelassene Arzt, seine Praxis wäre zu klein, um in den Fokus von Cyberkriminellen zu geraten. Doch auch in der Niederlassung drohen Cyberangriffe. Laut GDV sind gerade niedergelassene Ärzte ein interessantes Ziel für Cyberangriffe: Sie verfügen über sensible Patientendaten, die sie für Behandlungen, Dokumentationen und Abrechnungen unbedingt benötigen und schützen müssen, gelten als kreditwürdig und müssen als Selbständige auf ihre Reputation bedacht sein. All das macht sie erpressbar. Außerdem unterschätzen viele Ärzte noch immer die Bedeutung eines umfassenden Systems zur Cybersicherheit, sodass ihre Praxen technisch leicht angreifbar sind.

Besonders vielversprechend für Cyberkriminelle sind Attacken mit sogenannter Ransomware. Dabei verschaffen sich die Hacker Zugang zum Praxissystem und blockieren wichtige Funktionen oder stehlen Patientendaten. Den Zugang zu den Daten wollen die Hacker erst gegen eine Lösegeldzahlung wiederherstellen oder drohen sogar damit, Patientendaten zu veröffentlichen. Solche Angriffe beschränken sich laut Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht nur auf Industrieunternehmen, sondern treffen auch kleinere, weniger professionell geschützte Unternehmen.

Selbst wenn das Lösegeld nicht gezahlt wird, drohen durch solche Attacken erhebliche finanzielle Einbußen. Der GDI rechnet allein für Anwaltskosten, Informierung von Patienten und Datenschutzbehörden, Betriebsausfall und IT-Forensik mit Kosten von knapp 20 000 Euro. Werden tatsächlich Patientendaten veröffentlicht, können Schadenersatzzahlungen an Patienten fällig werden. Diese können laut GDI im 5-stelligen Bereich liegen.

Schwachstelle Personal – wie Cyberkriminelle arbeiten

Die meisten Ärzte lassen ihre Netzwerke von IT-Profis absichern. Doch im Alltag verwenden viele Praxen zu simple Passwörter über zu lange Zeiträume oder verzichten darauf, neue Verschlüsselungssoftwares zu nutzen. Das nutzen die Hacker und dringen über Schadsoftwares in E-Mail-Anhängen bzw. über Links, die in E-Mails eingebettet sind, in das Praxisnetzwerk ein.

Einen ersten Einblick verschaffen Hacker sich oft anhand spezieller Suchmaschinen.

Mit dem Internetdienst Shodan etwa kann man gezielt nach angreifbaren Geräten im Internet suchen. Haben Kriminelle auf diese Weise ein Opfer ausgemacht, setzen sie häufig sogenannte Social-Engineering-Techniken ein, um an vertrauliche Daten zu kommen, die ihnen den Zugang erleichtern. Dazu kontaktieren sie Mitarbeiter und bauen einen freundlichen, persönlichen Kontakt zu ihnen auf.

Im vermeintlich privaten Gespräch entlocken sie ihnen dann wichtige Daten, anhand derer sie Passwörter erraten oder anderen Zugang zum Netzwerk finden. Manche Gauner kommen auch persönlich auf einen Plausch vorbei und lassen etwa am Empfang „zufällig“ einen USB-Stick mit einer Spionagesoftware liegen. Um den Besitzer herauszufinden, schließen Mitarbeiter solche USB-Sticks häufig kurz an. Ab diesem Moment haben die Kriminellen freien Zugang zum Praxisnetzwerk.

IT-Experten empfehlen deshalb, als womöglich wichtigsten Schritt zur Cybersicherheit, alle Mitarbeiter regelmäßig zu Social-Engineering-Techniken zu schulen. „Die wichtigste Voraussetzung für alle Maßnahmen ist ein grundlegendes Bewusstsein der Mitarbeiter für die Gefährdung der eigenen IT-Infrastruktur“, schreibt der ZVEI Zentralverband Elektrotechnik- und Elektroindustrie e.V. deshalb auf seiner Website.

Cybersabotage – wenn Kriminelle medizinische Geräte beeinflussen

Datenklau ist nicht die einzige Gefahr für Arztpraxen. Cyberkriminelle können z. B. medizinische Geräte hacken und sie von außen steuern. Infusionspumpen, Beatmungsgeräte, implantierbare Herzschrittmacher oder Defibrillatoren, Kühlsysteme für Blutkonserven oder bildgebende Systeme sind potenzielle Angriffsziele. Leider sind Medizingeräte ausgerechnet aufgrund von Sicherheitsstandards anfälliger für Angriffe als viele andere Anlagen.

Dieses Paradoxon kommt so zustande: Weil die Anforderungen an die Sicherheit beim Betreiben von Medizingeräten besonders hoch sind, sind eigentlich unverzichtbare Software-Updates nicht ohne weiteres möglich. Den Grund dafür erklärt der Zentralverband Elektrotechnik- und Elektroindustrie e. V. (ZVEI): „Bei Software-Updates muss der Hersteller überprüfen, ob sich durch die Anpassung der Software neue Aspekte ergeben, welche die Sicherheit oder den bestimmungsgemäßen Gebrauch des Medizinprodukts verändern. Das gilt auch für eine Anti-Viren-Software, da diese möglicherweise die Funktionen des Medizinprodukts beeinflussen kann.

Akt Rheumatol 2021; 46: 128–129

Eine neue Software darf deshalb erst dann auf Medizinprodukte aufgespielt werden, wenn der Hersteller die Software nach einer gründlichen Überprüfung freigegeben hat. Regelmäßige automatische Updates können hier deshalb oft noch nicht zum Einsatz kommen". Praktisch ist es also wahrscheinlich, dass ein Sicherheitsupdate erst dann genehmigt wird, wenn bereits neue, durch das inzwischen veraltete Update noch nicht erfasste Schadsoftware im Umlauf ist.

Ein weiterer kritischer Punkt: Medizintechnische Geräte und Anlagen in Arztpraxen sind häufig permanent mit dem Internet verbunden. Hersteller müssen deshalb künftig noch mehr Anforderungen an die Cybersicherheit in Bezug auf Programmierung, Prüfung, Implementierung und After-Sales-Pflege der Software umsetzen. Das allerdings setzt auch eine passgenauere Abstimmung auf die geplante Betriebsumgebung und die geplante Verwendung voraus, also eine Zusammenarbeit zwischen dem Hersteller und dem künftigen Betreiber, dem Arzt.

Auch Fachsoftware könnte grundsätzlich ein Einfallstor für Cyberkriminelle darstellen. Etwa könnten über im medizinischen Bilddatenmanagement verbreitete, offene Kommunikationsstandards wie DICOM (Digital Imaging and Communications in Medicine; deutsch: Digitale Bildgebung und -kommunikation in der Medizin) auch radiologische Aufnahmen manipuliert oder Schadsoftware verbreitet werden. Laut dem Zentralverband der Elektrotechnik- und Elektroindustrie e. V. (ZVEI) sind hier bisher keine gezielten Angriffe bekannt, allerdings sei eine Diskussion über mögliche technische Schwachstellen in diesem Bereich wichtig.

Tipps für den Schutz vor Cyberangriffen

Der GDV zeigt in seinem Branchenbericht, dass die meisten Praxen unzureichend gegen Cyberattacken geschützt sind, etwa zu einfache Passwörter nutzen, diese zu selten wechseln und bei der Mail-Verschlüsselung nicht auf dem neuesten Stand der Technik sind. Dennoch sei die Mehrheit der Praxisinhaber davon überzeugt, gut vor Cyberangriffen geschützt zu sein.

Die Experten vom GDV raten, beim Thema Cybersicherheit mindestens diese 10 Punkte zu beachten:

1. Regelmäßig Sofwareupdates durchführen.
2. Mindestens 1-mal wöchentlich Sicherungskopien machen.
3. Administratoren-Rechte nur an Administratoren vergeben.
4. Systeme, die über das Internet erreichbar oder im mobilen Einsatz sind, zusätzlich durch 2-Faktor-Authentifizierung schützen.
5. Manipulation und unberechtigten Zugriff auf Sicherungskopien verhindern.
6. Schutz gegen Schadsoftware installieren (Virenscanner usw., regelmäßig updaten!).
7. Sicherungskopien physisch vom gesicherten System trennen.
8. Mindestanforderungen für Passwörter einhalten.
9. Individuelle Kennungen und Passwörter für jeden Nutzer vergeben.
10. Wiederherstellung von Daten aus Sicherungskopie regelmäßig testen.

Einige Versicherer bieten Policen für Ärzte zum Schutz vor Cyberangriffen. Der Abschluss einer solchen Versicherung hat den Vorteil, dass die Anbieter meist einen jeweils aktuellen Katalog an Maßnahmen vorschreiben, um das Risiko eines Angriffs zu senken. Ein solcher Maßnahmenkatalog ist ein guter Ausgangspunkt für ein eigenes Sicherheitssystem.

Ob versichert oder nicht – wenn es zu einer Attacke kommt, sollte man unbedingt Anzeige erstatten und mit Polizei und Behörden kooperieren.

Eine andere Möglichkeit, ein eigenes Cybersicherheitsprogramm aufzustellen: Medizingerätehersteller wie etwa Dräger beraten und trainieren ihre Kunden auch zum Thema Cybersicherheit.

Marisa Kurz, München

Zitierweise für diesen Artikel

Dtsch Med Wochenschr 2019; 144: 1591–1592. doi:10.1055/a-0979-1055