Bedrohung so hoch wie nie – NIS2 soll's richten

???? - stock.adobe.com

IT-Sicherheit *Ransomware und andere Angriffsmethoden gefährden weiterhin Krankenhäuser, Pflegeeinrichtungen und Co. Mit der NIS2-Richtlinie will die EU die Schutzmechanismen verstärken.*

Text: Arno Laxy.

Lindenbrunn, Lippstadt, Erwitte und Gesecke – diese Ortsnamen stehen für jüngste Attacken von Cyber-Kriminellen auf Krankenhäuser. Anfang Februar ist das Krankenhaus Lindenbrunn in Coppenbrügge in Niedersachsen gemeinsam mit angeschlossenen Pflegeeinrichtungen Ziel eines Cyber-

matthias.heinz@medtrix.group

Angriffs geworden ist. Ebenfalls um diese Zeit herum erwischte es die IT-Infrastruktur des Dreifaltigkeits-Hospitals in Lippstadt, mit angeschlossenen Häusern in Erwitte und Gesecke.

Das Gesundheitswesen gehört weiterhin zu den bevorzugten Zielen der Cyber-Kriminellen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schätzt in seinem Infobrief vom Februar 2024 „die Bedrohungslage im Gesundheitswesen aktuell so hoch ein wie nie".

„Die Angriffsmethoden werden nicht zuletzt durch Künstliche Intelligenz (KI) immer vielfältiger."

Im Lagebericht vom November 2023 hatte sich das BSI generell mit der Thematik beschäftigt und im „Berichtszeitraum eine angespannte bis kritische Lage" konstatiert. Insgesamt hat die Behörde für den Zeitraum 2022-2023 132 Meldungen zu Cyberattacken aus dem Gesundheitssektor erhalten. „Wie schon in den vergangenen Jahren wurde eine hohe Bedrohung durch Cyberkriminalität beobachtet. Ransomware blieb die Hauptbedrohung."

Mit Ransomware (Erpressertrojaner) wird bekanntlich eine Software bezeichnet, über die IT-Systeme infiltriert und verschlüsselt werden können, um anschließend für die Wiederherausgabe der Daten ein Lösegeld zu verlangen. Weltweit haben Ransomware-Erpresser im letzten Jahr laut einer Studie des Blockchain-Analyseunternehmens Chainalysis 1,1 Milliarden US-Dollar eingenommen, fast doppelt so viel wie im Vorjahr.

Dabei werden die Angriffsmethoden nicht zuletzt durch Künstliche Intelligenz (KI) immer vielfältiger. Einer der Hauptangriffswege auf Einrichtungen des Gesundheitswesens ist die E-Mail, so Experten. Für die überzeugendsten E-Mail-Angriffe fälschen Cyberkriminelle die E-Mail-Adresse einer Organisation, zu der

ihr Opfer bereits eine Geschäftsbeziehung unterhält. Hierbei kommt ihnen die KI zu Hilfe. Angreifer verwenden sie, um z.B. täuschend echte E-Mails mit gefälschten Rechnungen über gehackte E-Mail-Konten zu verfassen, die nur schwer von echten Nachrichten zu unterscheiden sind. Oft genug bringen sie die Adressaten dazu, auf gefälschte Konten einzuzahlen.

In die gleiche Richtung gehen Angriffe mit Hilfe der Deep-Fake-Technologie. Diese ermöglicht es, Stimmen und Anrufe so zu manipulieren, dass sie täuschend echt klingen. Angreifer können sich z.B. als Mitarbeiter eines Unternehmens ausgeben, um an sensible Informationen zu gelangen. Auch nutzen sie wiederum die persönliche Beziehung zwischen Anbietern und ihren Kunden aus, um Vertrauen zu schaffen.

NIS 2 – mehr IT-Sicherheit per EU-Richtlinie

Die IT-Sicherheit zu erhöhen, sowohl in Krankenhäusern als auch in anderen Organisationen, ist daher auch ein vordringliches Ziel nationaler und europäischer Gesetzgeber. Darum hat die EU auf die Gefahrenlage reagiert und eine umfassende Cybersicherheitsstrategie herausgebracht. Ein zentraler Bestandteil ist die Netz- und Informationssicherheitsrichtlinie 2.0 (NIS2), die am 16. Januar 2023 EU-weit Gültigkeit erlangt hat. Bis zum 18. Oktober 2024 muss ihre Umsetzung auf Ebene der EU-Länder in Gesetzesform geregelt sein. Im Kern zieht NIS2 die Anforderungen an die Cyber- und Informationssicherheit enger, besonders für Betreiber kritischer Infrastrukturen (KRITIS). Werden die Anforderungen der Richtlinie nicht erfüllt, wird die Geschäftsleitung in die Haftung genommen.

Damit Patientendaten und wichtige medizinische Infrastrukturen besser geschützt werden, müssen die Schutzmaßnahmen rasch erhöht werden. Darum setzt die EU mit ihrer Richtlinie auch klare Zeitvorgaben, verbunden mit empfindlichen Bußgeldern für Krankenhäuser, die sich nicht daran halten. Diese können bis zu zehn Millionen Euro oder zwei Prozent des Jahresumsatzes ausmachen. Zu den eingeforderten Maßnahmen zum Risikomanagement gehören die Identifizierung von Schwachstellen, die Überwachung des Netzwerks und die Schulung der Mitarbeiter.

Neben den in der Richtlinie verpflichtend benannten Maßnahmen, können Krankenhäuser noch andere Initiativen wie z.B. die Einführung von Multi-Faktor-Authentifizierung, Datenverschlüsselung, Backup- und Recovery-Lösungen sowie die Entwicklung eines Notfallplanes bei Cyberangriffen ergreifen, um ihre Cybersicherheit zu erhöhen.

NIS2 wird in den nächsten Wochen und Monaten sicherlich viele IT-Abteilungen von Krankenhäusern in Atem halten, denn bis Mitte Oktober bleibt nicht viel Zeit. Hinzu kommt, dass zum Redaktionsschluss dieses Beitrags immer noch einige Details, wie die nationalen Ausführungsbestimmungen, ungeklärt sind. Die neuen EU-weiten Bestimmungen werden sicherlich die gewünschten Effekte zeitigen und die IT-Sicherheit verbessern. Zu wünschen wäre, dass die notwendige nationale Rahmensetzung jetzt schnell erfolgt, damit Planungssicherheit für alle Beteiligten besteht.

Das sagt die DKG zur NIS2-Richtlinie

Auf Anfrage von Management & Krankenhaus hat Mar-

AZ

kus Holzbrecher-Morys, DKG-Geschäftsbereichsleiter Digitalisierung & eHealth in einem umfangreichen Statement die Position des Interessen- und Dachverbands von Spitzen- und Landesverbänden der Krankenhausträger dargelegt:

„Die Umsetzung sowohl der NIS2-Richtlinie im NIS2UmsuCG als auch der CER-Richtlinie im KRITIS-DachG wird die Anforderungen im Bereich Cyberschutz und Resilienz weiter erhöhen. Dabei soll eine Vereinheitlichung der Vorgaben für Betreiber kritischer Anlagen z.B. mit Blick auf die Identifikation der kritischen Infrastrukturen, der Meldewege und -pflichten sowie der Nachweise erfolgen. Die Deutsche Krankenhausgesellschaft begrüßt ausdrücklich, dass hier Synergieeffekte genutzt werden sollen. Damit kann weiterer bürokratischer Aufwand vermieden werden.

Doch obwohl beide Gesetze im Oktober 2024 in Kraft treten sollen, sind gegenwärtig noch keine Termine für den weiteren Gesetzgebungsprozess bekannt. Dies dürfte die für die Umsetzung notwendige Vorlaufzeit weiter verkürzen. Erwartet wird nach den bisherigen Referentenentwürfen für beide Gesetze eine weitere Verbändeanhörung.

Bereits heute gelten für alle Krankenhäuser gesetzliche Anforderungen im Bereich Informationssicherheit. Mit den geplanten neuen Kategorien „Besonders wichtige Einrichtungen“ und „Wichtige Einrichtungen“ dürfte sich jedoch nicht nur die Zahl der betroffenen Einrichtungen in Deutschland über alle Sektoren und Branchen hinweg mindestens verzehnfachen, künftig werden praktisch alle Krankenhäuser unter die Regelungen zu Maßnahmen für Informationssicherheit, Registrierung und der Meldung von Vorfällen fallen. Und auch bei Nutzung vorhandener Meldeplattformen ist ein umfangreicheres Meldewesen mit Erstmeldung innerhalb von 24h sowie einer ausführlichen Zweitmeldung spätestens nach 72h geplant. Dies wird vermutlich trotz aller gegenteiligen Bemühungen den bürokratischen Aufwand durch Registrierung und Verarbeitung von Meldungen für Krankenhäuser stark erhöhen.

???? - stock.adobe.com

Ismodolore faciduisci tat nit at. Ut pratem quat nos ercin ecte te dolortie tie tat vullaore verit irit lut auguer

> *„Es gelten bereits für alle Krankenhäuser gesetzliche Anforderungen im Bereich Informationssicherheit.“*

Nach wie vor werden die Besonderheiten des Gesundheitsbereichs weder in den Begriffsdefinitionen noch den normativen Mindestvorgaben ausreichend adressiert, man denke hier an Themen, wie Lieferkettenkontrolle oder den Beschlagnahmeschutz. Und schließlich dürfte die enorme Ausweitung der Befugnisse des BSI ohne sektorspezifische Kontrollmechanismen – die für die Krankenhäuser zuständigen Landesbehörden werden nach dem aktuellen Gesetzentwurf kein qualifiziertes Mitspracherecht erhalten – zu noch stärkeren Friktionen führen, als es im Moment ohnehin der Fall ist. Wenn das BSI auch gegenüber „Besonders wichtigen Einrichtungen“ verbindliche Anweisungen zur Umsetzung der Verpflichtungen nach diesem Gesetz erlassen darf, ohne sich mit zuständigen Stellen auf Ebene der Länder – die ja für die Investitionsfinanzierung der Krankenhäuser zuständig sind – abstimmen zu müssen, wird der Streit um die Finanzierung der Maßnahmen auf dem Rücken der Krankenhäuser ausgetragen, obwohl überhaupt kein Zielkonflikt besteht: Die Informationssicherheit so gut wie möglich abzubilden und sich vor Cyberangriffen zu schützen, liegt im ureigenen Interesse eines jeden Krankenhauses.

Daher bleiben die Empfehlungen der DKG bestehen, dem Thema Informationssicherheit bei aller Brisanz der generellen weiteren Ausgestaltung der Krankenhauslandschaft in Deutschland das notwendige Maß an Aufmerksamkeit zu widmen. Die DKG stellt hierfür seit Jahren konkrete Informationsangebote und Arbeitsmittel in Form von Dokumentenpaketen für die Umsetzung der gesetzlichen Anforderungen bereit, insbesondere hat die DKG den für Betreiber kritischer Infrastrukturen empfohlenen Branchenspezifischen Sicherheitsstandard (B3S) für Krankenhäuser gemeinsam mit Experten aus den Bereichen medizinischer Versorgung und Informationssicherheit erstellt und passt diesen laufend an neue gesetzliche Anforderungen oder die sich verändernde Bedrohungslage an.“

Redaktion: 0611/9746405

Der Beitrag ist erstmals erschienen in: https://www.management-krankenhaus.de/news/it-sicherheit-bedrohungslage-hoch-wie-nie-nis2-solls-richten

privat

Kontakt

Arno Laxy
Journalist und PR-Berater
München
E-Mail: info@laxy.de