IT-Sicherheit

Frisches Geld für eine Dauerbaustelle

Krankenhäuser rücken immer häufiger ins Visier von Cyberkriminellen. Das Krankenhauszukunftsgesetz trägt dieser Gefahr Rechnung, die Förderrichtlinie ist allerdings hartes Brot und die Antragsstellung dürfte bei Kliniken für einiges Kopfzerbrechen sorgen.

Von Christina Spies

Ein Blick in den Bericht zur Lage der IT-Sicherheit in Deutschland 2020 macht deutlich: Cyberangriffe mit Schadsoftware – in immer neuen Varianten und mit teils ausgefeilten Methoden – prägen die aktuelle Gefährdungslage. So lautet das Ergebnis im Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die sogenannte Ransomware stellt demnach seit Jahren eine der größten Bedrohungen dar. Erst im September 2020 war das Uniklinikum Düsseldorf gezwungen, sich mehrere Tage von der Notfallversorgung abzumelden, weil Hacker sich über eine Sicherheitslücke Zugriff aufs System verschafft hatten (Seite 91). Die Lücke klaffte in einer „marktüblichen und weltweit verbreiteten kommerziellen Zusatzsoftware“, wie es seitens der Klinik heißt. Für die Betroffenen war der Hergang dramatisch: Die Systeme fielen nach und nach aus, Zugriffe auf gespeicherte Daten waren nicht mehr möglich. Ähnlich erging es im vergangenen Jahr dem Klinikum Fürth: Es konnte vorübergehend keine neuen Patienten mehr aufnehmen und musste Operationen verschieben, nachdem es zu einem Hackerangriff auf das IT-System gekommen war.

Insgesamt registrierte die Bundesregierung bis Anfang November 43 erfolgreiche Angriffe auf Gesundheitsdienstleister, das geht aus einer Antwort der Bundesregierung auf eine Anfrage der FDP im Bundestag hervor. Das seien mehr als doppelt so viele wie im gesamten vergangenen Jahr. Dass Kran-

Foto: Getty Images/Intpro

kenhäuser explizit auf der Angriffsliste von Cyberkriminellen stehen, könne man jedoch nicht sagen, teilt BSI-Pressesprecherin Josephine Steffen auf *f&w*-Anfrage mit. „Diese haben in der Regel ein Ziel: Geld. Beispielsweise durch Erpressung." Dafür werfen sie viele Köder aus, also in diesem Fall Schadsoftware, so dass möglichst viele Fische anbeißen. „Das kann dann ein Krankenhaus sein", erklärt Steffen. Dass es Cyberkriminelle gibt, die gezielter gegen Krankenhäuser vorgehen, schließt sie dennoch nicht aus. „Deshalb ist es gut, dass sich Krankenhäuser hier bislang gut aufgestellt haben und mit dem Krankenhauszukunftsgesetz ein echtes Novum geschaffen wurde."

Ständiger Wettlauf gegen die Zeit

Das KHZG sieht elf förderfähige Bereiche vor. Werden Mittel bewilligt, müssen mindestens 15 Prozent davon in die Verbesserung der IT-Sicherheit fließen. Beispiele sind unter anderem die Einführung eines Tools zum IT-Schwachstellenmanagement, ein Information Security Management System (ISMS) oder ein Sandbox-System, sagt Bernd Christoph Meisheit, IT-Chef des Klinikkonzerns Sana. Auch Herbert Motzel, Leiter der Stabsstelle IT-Sicherheitssysteme und -Strategie (CISO) am Klinikum Fürth, geht davon aus, dass die 15 Prozent hauptsächlich für den Schutz vor Hackerangriffen eingesetzt werden, beispielsweise für Virenschutz, Firewall oder die sogenannte Netzwerksegmentierung, die es ermöglicht, Viren – haben sie einen Bereich im Krankenhaus erreicht – einzudämmen und so die anderen Bereiche zu schützen. Auch Schulungen für Mitarbeiter seien notwendig, denn eine 100-prozentige technische Sicherheit sei nie möglich. Claudia Möller, Leiterin Zentraler Dienst FuE & Innovationsmanagement bei Agaplesion, vermutet, dass Krankenhäuser insgesamt ähnliche Projekte einreichen werden, da einige Fördertatbestände ab 2024 abschlagspflichtig sind und alle Einrichtungen deswegen versuchen werden, die Muss-Kriterien zu erfüllen.

Förderrichtlinien sind nie trivial, aber diese hat es wirklich in sich. Das KHZG sei ein vielversprechender Beginn, die hohen Anforderungen seien jedoch kaum zu erfüllen, sagt etwa der Bundesverband der Krankenhaus-IT-Leiter (Seite 94). Der Zeitplan sei eng getaktet und für manche Anforderungen gebe es noch keine Lösungen am Markt.

Möller schätzt das KHZG grundsätzlich als Chance ein. „Allerdings sind die in einigen Fördertatbeständen beschriebenen Muss-Kriterien sehr umfassend und nur schwer zu erfüllen", sagt sie. Auch wirken ihr Meinung nach manche Anforderungen stark anbietergetrieben. Darüber hinaus werden die durch das Gesetz zu etablierenden Lösungen nur über drei Jahre finanziert. Das müssen Kliniken beachten. Die danach teilweise sehr hohen laufenden Kosten für Schnittstellen, Lizenzen und Wartung müssen nach diesem Finanzierungszeitraum von den Krankenhäusern auch weiterfinanziert werden können. Es zeichnet sich bereits jetzt ab, dass einige Bundesländer die 30 Prozent des Finanzierungsanteils nicht vollständig tragen werden. „In Hessen beispielsweise müssen die Einrichtungen also mindestens 15 Prozent Eigenanteil an den Förderkosten tragen", sagt Möller. „Hier fehlt uns aktuell noch der langfristige Blick der Politik." Unklar ist teilweise auch noch, wie die 15 Prozent der IT-Sicherheitskosten pro Förderprojekt nachgewiesen werden können.

Sana-IT-Chef Meisheit ist voll des Lobes für das KHZG. „Es ist genau der richtige Weg", sagt er und ergänzt im selben Atemzug: „Es wird aber nicht ausreichen, IT-Sicherheit ist ein ständiger Wettlauf gegen die Zeit und das Aufrüsten der Angreifer." Bei Schutzsoftware handele es sich um handverlesene Werkzeuge von Herstellern, die regelmäßig auf den neusten Stand gebracht werden müssten – und das sei teuer, so Meisheit.

Ein Grund zur Panik sei das jedoch nicht. Häuser sollten einen Notfallplan in der Schublade haben, der vorgibt, was man bei einem Cyberangriff abschaltet und was nicht; und sie sollten ihn vorher testen. „So lässt sich lernen, was überhaupt der richtige Plan ist, um die Versorgung schnellstmöglich wieder hochzufahren." Wichtig sei, IT-Sicherheit nicht nur als ein notwendiges Übel zu betrachten, sondern als selbstverständlich, appelliert der IT-Chef. „Am besten ist es, wenn Häuser sich bei diesen Themen zusammenschließen und IT-Verbündete suchen, auch wenn sie im Wettbewerb stehen."

Herbert Motzel hält das KHZG ebenfalls für ein gutes Signal, die Investitionen von 15 Prozent in die IT-Sicherheit gingen in die richtige Richtung, sagt er. „Leider ist aber das Ziel, dass ‚privacy and security by design' sich im Stand der Technik widerspiegelt, noch nicht immer erreicht." Häufig stehe die Handhabbarkeit einer Softwarelösung an erster Stelle, die IT-Sicherheit komme erst zum Schluss. Damit stünden Betreiber häufig allein vor dem Problem, die vielen verschiedenen Angriffsflächen im Krankenhaus zu schützen. „Es wäre schöner, wenn es sich bei der IT-Sicherheit gleich um eine Produkteigenschaft handelt", sagt Motzel. In der Pflicht

Ransomware

Ransomware ist bereits seit einigen Jahren eine der größten Bedrohungen im Netz. Ist der Einsatz dieser Schadsoftware erfolgreich, verhindert sie den Zugriff auf lokale oder im Netzwerk erreichbare Daten und Systeme. Am häufigsten verschlüsseln die Hacker Nutzerdaten (wie Office-, Bild-, Ton- und Videodateien) oder ganze Datenbanken und fordern die Opfer dann auf, Lösegeld (Ransom) zu zahlen. Sie drohen mit Löschung oder Veröffentlichung der verschlüsselten Daten. Die Lösegeldzahlungen werden üblicherweise in digitalen Währungen (zum Beispiel Bitcoin) abgewickelt, um die Strafverfolgung zu erschweren. Ransomware wird über die bei Schadprogrammen üblichen Angriffsvektoren als E-Mail-Anhang oder als Link verbreitet, der auf eine infizierte Webseite führt. Einen Angriffsvektor, der speziell für Unternehmen und andere Einrichtungen mit größerer IT-Infrastruktur gefährlich ist, stellen Schwachstellen in Fernwartungs- und VPN-Zugängen dar.

KHZG: Auf einen Blick

Das Bundesministerium für Gesundheit (BMG) und das Bundesamt für Soziale Sicherung (BAS) haben Ende November die Förderrichtlinie zum Krankenhauszukunftsgesetz (KHZG) veröffentlicht.

- Über „Muss"- und „Kann"-Kriterien definiert sie die Anforderungen der elf im Gesetz benannten förderungsfähigen Vorhaben. Das zur Förderung beantragte Vorhaben darf frühestens am 2. September 2020 begonnen haben.
- Für alle Bereiche gilt, dass 15 Prozent des Fördergeldes in die IT-Sicherheit fließen müssen.
- Des Weiteren gilt für sechs der elf Bereiche die Interoperabilität digitaler Dienste als Voraussetzung. Nur dann sind die Vorhaben förderfähig.
- 4,3 Milliarden Euro sollen in die Digitalisierung der Krankenhäuser fließen. Der Bund übernimmt 70 Prozent der Kosten für die entsprechenden Projekte. 30 Prozent sollen die Länder und/oder die Krankenhausträger zuschießen. Der sogenannte Königsteiner Schlüssel begrenzt die Summe der möglichen Förderung durch das Bundesland.
- Das Krankenhaus erstellt mithilfe des Formulars, zu finden auf der Homepage des BAS, eine Bedarfsanmeldung. Das Land hat drei Monate Zeit, um über die Förderung zu entscheiden und anschließend einen Antrag beim BAS zu stellen. Sie müssen ihre Anträge gegenüber dem BAS bis spätestens zum 31. Dezember 2021 gestellt haben, heißt es in der Richtlinie. Das BAS prüft die Anträge der Länder, entscheidet, welche Projekte gefördert werden sollen, und zahlt die Fördergelder an das Land aus, welches die Gelder an die Krankenhausträger weiterleiten soll.
- Will ein Krankenhaus einen Antrag einreichen, braucht es einen Nachweis hinsichtlich der „notwendigen Eignung" eines IT-Dienstleisters, der eine Berechtigung vom BAS erteilt bekommen hat. Die notwendige Eignung ist durch das Absolvieren eines Schulungsprogramms zu erlangen. Das Schulungsprogramm gestaltet das BAS und stellt es ab dem 1. Januar 2021 auf der Homepage unter www.bundesamtsozialesicherung.de kostenlos zur Verfügung.

Auf einer Veranstaltung des Health Innovation Hub sagte Thomas Süptitz, Leiter des Referats Cybersicherheit und Interoperabilität im BMG: „Die Möglichkeit, sich berechtigen zu lassen, steht jedem offen." Mit der Zertifizierung wolle man Sicherheit erreichen, damit die Anträge, die gestellt werden, inhaltlich gut und damit förderungsfähig sind.

- Das BMG will bis zum 28. Februar 2021 eine Forschungseinrichtung mit einer den Krankenhauszukunftsfonds begleitenden Auswertung beauftragen: Zum 30. Juni 2021 und zum 30. Juni 2023 wird dafür der Reifegrad aller Krankenhäuser evaluiert. Der Bundesverband der Krankenhaus-IT-Leiter empfiehlt, sich noch nicht auf eine Methode für die Ermittlung des Digitalisierungsgrades festzulegen, sondern konkrete Projekte zu planen, für die Häuser einen Antrag stellen wollen.
- Krankenhäuser, deren digitaler Reifegrad nicht den Anforderungen genügt, drohen ab dem 1. Januar 2025 Abschläge von zwei Prozent auf Patientenrechnungen.

sieht der Chief Information Security Officer jedoch nicht die Hersteller allein: Nur gemeinsam durch Politik, Hersteller und Betreiber könnten Hackerangriffe wirksam angegangen werden. Verbesserungen werde vor allem das IT-Sicherheitsgesetz 2.0 bringen, ist Motzel überzeugt, denn es sehe laut einem Referentenentwurf vor, dem BSI mehr Befugnisse einzuräumen und Herstellern Mindeststandards vorzugeben.

Einrichtungen der Kritischen Infrastruktur (Kritis) hat das BSI ebenfalls im Blick. Zur Umsetzung der Kritis-Verordnung wurden zwischenzeitlich Leitlinien und Standards wie der B3S der Deutschen Krankenhausgesellschaft oder der Anforderungskatalog für Kritis-Betreiber des BSI entwickelt, um Hackerangriffen zu begegnen.

Derzeit gelten jedoch nur Krankenhäuser mit mehr als 30.000 stationären Fällen pro Jahr als Kritis-Einrichtungen. Gerüchten zufolge soll das BSI an einer zum IT-Sicherheitsgesetz ergänzenden Kritis-Verordnung arbeiten. Unter anderem heißt es, dass der Schwellenwert von aktuell 30.000 stationären Fällen im Jahr herabgesenkt werden soll. Das BSI nimmt bis Redaktionsschluss jedoch keine Stellung, aufgrund der laufenden Abstimmungen des „sich derzeit in der Ressortabstimmung befindenden Referentenentwurfs zum IT-Sicherheitsgesetz 2.0".

Insellösungen miteinander verbinden

Einen weiteren Fokus legt die Förderrichtlinie neben der IT-Sicherheit auf die Interoperabilität. Gleich mehrere Vorhaben sind nur dann förderfähig, wenn dabei auf „international anerkannte technische, syntaktische und semantische Standards" zurückgegriffen wird, heißt es in dem Papier. Bedeutet also: Dem Gesetzgeber ist es ein Anliegen, Medienbrüche im Sinne der Patientensicherheit sektorenübergreifend zu vermeiden. Der KH-IT begrüßt das. Damit könne langfristig die Abhängigkeit von den wenigen KIS-Herstellern verringert werden und das Krankenhaus wird wieder Herr seiner eigenen Daten werden. Auch Möller findet es gut, dass das Thema mehr in den Vordergrund gerückt wird: „Daten müssen ohne große Zusatzkosten für Schnittstellen in andere Systeme oder in die eigene IT-Infrastruktur übertragbar sein."

Wie man Interoperabilität digitaler Dienste erzeugt, beschreibt die Förderrichtlinie ebenfalls. Als Standard sieht sie die über die KBV definierten Medizinischen Informationsobjekte (MIO) beziehungsweise das Interoperabilitätsverzeichnis der Gematik (Vesta) vor. Sofern diese beiden nicht vorhanden sind, gibt es die Möglichkeit, eine entsprechende Lösung über einen existierenden offenen, international anerkannten Schnittstellen- und/oder Interoperabilitätsstandard umzusetzen. Ausdrücklich ist beispielsweise FHIR genannt. Weiter gelten als offene, international anerkannte Standards unter anderem auch LOINC und Snomed-CT.