Hört auf Euch zu beschweren!

„Vorsorge ist besser als Nachsorge“ – das gilt nicht nur für die menschliche Gesundheit, sondern auch für das unternehmerische Wohlergehen von Kliniken und anderen Leistungserbringer:innen. Zahlreiche Vorfälle aus der Vergangenheit zeigen, wie fatal die Auswirkungen eines Cyberangriffs auf die komplette Versorgungskette sind.

Text: Nina Khan

Wie gefährdet eine Organisation ist und wie hoch der potenzielle Schaden im Ernstfall wird, kann im Vorfeld im Rahmen des Business Continuity Managements (BCM) ermittelt werden. Die Erkenntnisse dienen der Maßnahmenplanung für die Aufrechterhaltung des Betriebs trotz Notfallsituation.

Besonders im Gesundheitswesen ist die Gefährdung von sensiblen Informationen und Prozessen aufgrund der Kritikalität als Leistungserbringer:in durch einen Cyberangriff mit drastischen Folgen verbunden – die Informationssicherheit in Digitalisierungsprojekten muss deshalb von Beginn an zum Standard werden.

Stattdessen sind die Beschwerden nach wie vor laut, Informationssicherheit und Datenschutz gelten als Verhinderer und als Grund für das Scheitern der Projekte - ein unsachgemäßer Vorwurf, der sich jedoch hartnäckig hält.

Das Jahr 2022 neigte sich bereits dem Ende zu, als die Meldung aus dem Klinikum Lippe sämtlichen Akteuren aus dem Gesundheitswesen den Atem stocken ließ: Ein massiver Cyberangriff führte zu Teilausfällen der IT an allen drei Standorten in Detmold, Lemgo und Bad Salzuflen. Das Landeskriminalamt, Ermittelnde aus Bielefeld und Köln, externe Cybersicherheits-Dienstleister:innen sowie eine Wirtschaftsprüfungsgesellschaft schritten ein, um gemeinsam durch Abwehrmaßnahmen den Angriff abzuwenden. Später hieß es, dass die Entschlüsselung der Systeme durch intensive Verhandlungen mit den Erpresseri:innen gelungen sei. Die IT-Infrastruktur wurde heruntergefahren, IT-Systeme neu aufgesetzt. Zwei Wochen lang konnte das Klinikum nur per Telefon oder Fax kontaktiert werden. Allerdings seien zu keiner Zeit Patient:innen gefährdet gewesen.

Anders war das bei einem Angriff zwei Jahre zuvor auf eines der größten Krankenhäuser in Nordrhein-Westfalen, dem Universitätsklinikum Düsseldorf, bei dem Daten von 30 Servern durch Hacker verschlüsselt wurden. Die Folge war das Albtraumszenario eines jeden Klinikums: Operationen und Behandlungen fielen aus, Ambulanzen und Notaufnahmen mussten schließen. Aus einem Erpresserschreiben ging hervor, dass die Attacke eigentlich der Heinrich-Heine-Universität galt. Nachdem die Ermittler:innen den Hackern mitteilten, ein falsches Angriffsziel getroffen zu haben, wurde der Entschlüsselungscode kommuniziert. Dennoch dauerte es mehrere Wochen, bis der Krankenhausbetrieb wieder normal lief. Frank Schneider, der Ärztliche Direktor der Klinik, teilte dem WDR damals mit:

> Keine Notarztwagen, keine Hubschrauber, keine Krankenwagen kamen mehr, alle Ambulanzen waren geschlossen. Das ist eine schreckliche Zeit gewesen für uns und die Patient:innen.

Die Liste der Cyberangriffe lässt sich im jungen Jahr 2023 problemlos weiterführen: Der Dienstleister von Sozialversicherungsträgern BITMARCK bestätigte im Januar den unbefugten Zugriff auf die IT-Infrastruktur, ebenso wie der IT-Dienstleister adesso. Kurz darauf berichteten Medien von einer globalen Hackerattacke durch eine IT-Sicherheitslücke, bei der Hunderte Firmen, darunter auch deutsche, von Erpressersoftware betroffen waren.

Höher, weiter, Ransomware

Während Künstliche Intelligenz die Medizin revolutioniert, beispielsweise durch die Analyse von Röntgen und Ultraschallbildern und KI-Projekte damit weitreichenden Einfluss in die Diagnostik und den Behandlungsverlauf nehmen, sind Informations- und IT-Sicherheit die unliebsamen Stiefschwestern der Digitalisierungsprojekte. Selbiges gilt für Dienstleister:innen und Leistungserbringer:innen. Scharfe Social-Media-Slogans wie „Tod dem Datenschutz“ machen deutlich, dass Datenschutz immer noch als Bremsklotz betrachtet und Datenschutzbeauftragte als Verhindernde tituliert werden. „Das ist allerdings falsch“, macht Prof. Dr. Thomas Jäschke, Medizininformatiker und Professor für Wirtschaftsinformatik, klar.

> Ja, der DSB hat die Aufgabe zu kontrollieren. **Er hat aber vor allem auch die Aufgabe zu gestalten und zu beraten.**

Insofern sind Datenschutzbeauftragte auch Datenschutzberater:innen, die dabei helfen, die Projekte umzusetzen. Denn Lösungen sind vorhanden. Diese mögen Arbeit machen und Geld kosten, aber am Ende des Tages sprechen wir von einer wesentlichen Erhöhung der Sicherheit. Ich lade dazu ein, die ständigen Beschwerden über den Datenschutz einzustellen und stattdessen nach vorne zu blicken.

Der Blick nach vorne soll vor allem durch das Krankenhauszukunftsgesetz (KHZG) ermöglicht werden. Es stellt mit einem Fördervolumen von insgesamt 4,3 Milliarden Euro den größten Treiber dar, um den Digitalisierungsgrad zu erhöhen. Bei bewilligten Projekten müssen 15 Prozent der geförderten Summe für IT-Security und Informationssicherheit aufgewendet werden.

Bis die ersten Projekte aber messbare Erfolge erzielen, werden noch Jahre vergehen. Daher ist es keine Überraschung, dass das Bundesamt für Sicherheit und Informationstechnik (BSI) in seinem aktuellen Lagebericht von 2022 Alarm schlägt, dass die Gefährdungslage im Cyber-Raum so hoch war wie nie zuvor. Die digitale Erpressung durch Ransomware-Angriffe stelle dabei die größte Bedrohung dar. Zu demselben Ergebnis kommt auch die Sophos-Studie „State of Ransomware 2022“: Das Marktforschungsunternehmen Vanson Bourne befragte für den britischen Softwarehersteller weltweit 5.600 IT-Experten zur Ransomware-Entwicklung in insgesamt 31 Ländern. Darunter befanden sich 63 IT-Leitungen aus Deutschland in dem Bereich Gesundheitswesen.

Insgesamt hat sich innerhalb von 12 Monaten die Anzahl von Ransomware-Angriffen der befragten Unternehmen von einem Drittel (37 Prozent) auf fast zwei Drittel (66 Prozent) verdoppelt. Es lässt sich nicht leugnen: Hacker, die Organisationen durch Ransomware manipulieren, verbuchen einen hohen Erfolg, Tendenz steigend. Das liegt unter anderem daran, dass sie immer niederschwelliger kompetent sein müssen, um einen Angriff durchzuführen und gleichzeitig eine relativ hohe Bereitschaft von Unternehmen zugrunde liegt, Lösegeld zu zahlen. Immerhin waren es insgesamt 46 Prozent der Unternehmen im Jahr 2022, die sich erpressen ließen. Das Gesundheitswesen gehört zwar zu den Branchen mit der geringsten Bereitschaft, Lösegeld zu zahlen; der Grund, dass es über weniger Budget als andere Branchen verfügt, ist allerdings eher pragmatischer Natur.

Hoher Digitalisierungsgrad, hohes Risiko

Es darf klar und deutlich gesagt werden: Ein Cyberangriff auf eine Klinik setzt Menschenleben aufs Spiel. SensibleInformationen wie der Behandlungsablauf von Patient:innen oder die Funktionalität von OP-Geräten sind bei steigendem Digitalisierungsgrad einem erhöhten Risiko auf unbefugte Zugriffe ausgesetzt. Ob Trojaner-, Phishing- oder Ransomware-Angriffe: Es ist längst bekannt, dass menschliches Fehlverhalten die größte Sicherheitslücke von IT-Systemen ist. Die Verschlüsselung von Daten wird stetig komplexer - der Risikofaktor Mensch wird daher auch in Zukunft das größte Einfallstor für Hacker bleiben, sodass Angriffe niemals komplett ausgeschlossen werden können. Genau hier kommt das Business Continuity Managements ins Spiel. Die Managementmethode definiert alle Prozesse, um als Betrieb im Ernstfall handlungsfähig zu bleiben.

Insbesondere in Kliniken sollte der Schutz von Informationen – also die Informationssicherheit – Priorität haben, vor allem, wenn es um die IT-Sicherheit vor Cyberangriffen geht. Einmal mehr gilt es, Informationssicherheit und Datenschutz von Beginn an mit einzubeziehen. „Gesetzliche Anforderungen wie Security und Privacy by Design sind in Digitalisierungsprojekten frühzeitig zu berücksichtigen“, erläutert Thomas Jäschke, „im Bereich der Informationssicherheit wird im Sinne des Business Continuity Managements das Fundament für erfolgreiche Digitalisierungsprojekte geschaffen. Sie sind essenziell für die erfolgreiche und sichere Digitalisierung.“ Das Vorgehen, das von Anfang an umgesetzt werden muss, ist das sogenannte Security Engineering.

Experten identifizieren die Informationen und Daten in den vorliegenden Prozessen eines Digitalisierungsprojektes, indem sie eine Schutzbedarfsanalyse durchführen. Sie überprüfen dabei Prozesse und Assets hinsichtlich der drei primären Schutzziele „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“.

Der Schutzbedarfsanalyse folgen die Gefährdungs- und Risikoanalyse, in denen besonders gefährdete Assets und Prozesse betrachtet werden. Mithilfe einer Risikoanalyse werden entsprechende Maßnahmen abgeleitet, die das Weiterführen des Betriebs trotz Notfallsituation gewährleisten.

Tipp: Lesen Sie mehr über die Schutzbedarfs,-Gefährdungs- und Risikoanalyse im nachfolgenden Artikel ab Seite 8.

Unternehmen müssen Risiken einkalkulieren und bis zu einem gewissen Maße akzeptieren, auch das ist Teil von Business Continuity Management. Notfallkonzepte dienen dann als weiterführende Maßnahme für den Fall der Fälle. „Es gibt keinen Standardplan für Business Continuity Management. Die Maßnahmen müssen individuell für jede Organisation entwickelt werden. Was aber übergreifend für alle gilt, ist die Gründung eines Incident Response Teams, das im Notfall kontaktiert wird, klar definierte Ablauf- und Notfallpläne und nicht zuletzt die Sensibilisierung des gesamten Personals“, fasst Thomas Jäschke zusammen.

In einem Krankenhaus öffnen nicht nur IT-Mitarbeitende eine E-Mail, sondern vom Pförtner über die Verwaltung bis zum Klinikdirektor auch alle anderen Mitarbeitenden und schließlich auch externe Leistungserbringer:innen. Damit besteht in jeder Abteilung und in jeder einzelnen E-Mail die potenzielle Gefahr, eine Klinik zu gefährden. Entgegenwirken kann dem ein präventives Vorgehen durch entsprechende Awarenessmaßnahmen. Als Digitalisierungsexperte mit 30-jähriger Erfahrung weiß Thomas Jäschke, dass davon alle Seiten profitieren: „Wenn Unternehmen in die Sicherheit durch qualifiziertes Personal investieren und die Security-Awareness bei Mitarbeitenden erhöhen, dann ist das für sie bei ihren Anwendungen auch im privaten Umfeld ein Wissensgewinn. Wer eine Phishing-Mail erkennt und um ihre Folgen weiß, wird sie erst recht nicht auf dem eigenen Rechner zu Hause öffnen. Der Nutzen für den Einzelnen wird schnell begreifbar und das wirkt sich wiederum positiv auf das Unternehmen aus.“

Digitalisierungsprojekte müssen holistisch gesteuert werden

Während auf der einen Seite die zunehmende Digitalisierung in der Medizin die Angriffsfläche für Cyberkriminalität vergrößert und Informationen einer immer höheren Gefährdung durch Cyberattacken ausgesetzt sind, ist auf der anderen Seite die Bereitschaft für Investitionen in Cyber-Security, Informationssicherheit und Datenschutz überaus gering. So liegen IT-Budgets im Gesundheitswesen für Sicherheitsvorkehrungen im Schnitt bei nur 10 Prozent. Gibt es hier ein Effizienz-Problem?

„Ja“, meint Thomas Jäschke, „die größte Herausforderung im Digitalisierungsprozess für Kliniken ist der akute Personalmangel, insbesondere in der Digitalisierung und der IT. Krankenhäuser kommen nicht drumherum, mit externen Partner:innen zusammenzuarbeiten, die auf den Punkt das Know-how liefern, das bei der Umsetzung der digitalen Transformation benötigt wird. Folglich müssen interne Mitarbeitende dazu befähigt werden, externe Ressourcen zu steuern und ein vernünftiges Multiprojektmanagement voranzutreiben.“

Die Sensibilisierung der Mitarbeitenden durch entsprechende Schulungen und die Investition in qualifiziertes Personal verdeutlichen, dass Informationssicherheit ein Thema für die Managementebene ist und von hier aus in den Betrieb getragen werden muss. Magnus Welz, Bereichsvorstand IT- und Wissensmanagement der DATATREE AG, spricht aus Erfahrung, denn er setzt seit 15 Jahren Informationssicherheits- und IT-Projekte mit Kund:innen um: „Das Bereitstellen und die Ernennung von Verantwortlichen ist ein wichtiger Aspekt bei der Umsetzung von Digitalisierungsprojekten. Es geht hierbei um ganzheitliche Prozessbetrachtung: Ein Chief Digital Officer (CDO) hat eine klar benannte Stelle inne, die offiziell die Verantwortung für den gesamten Digitalisierungsprozess übernimmt – und das ist wichtig. In vielen Kliniken ist es noch immer so, dass die IT-Abteilung als Treiber der Digitalisierung verstanden wird. Bei gleichzeitigem Ressourcenmangel ist den Mitarbeitenden aber meistens gar nicht möglich, die Projekte auch strategisch voranzutreiben. Die IT ist und bleibt essenziell für die Umsetzung von Digitalisierungsprojekten. Ihre Steuerung jedoch muss holistischer gestaltet werden.“

> **Die Sicherheit von Digitalisierungsprojekten beginnt immer vor dem Angriff.**

„Informationssicherheit und Datenschutz im Rahmen des Business Continuity Managements zu spät oder sogar gar nicht mit einzubeziehen ist wie Autofahren ohne Sicherheitsgurt oder wie Motorradfahren ohne Helm“, zieht Thomas Jäschke das Fazit, „das würde heutzutage schließlich auch niemand mehr machen. Wenn alle Akteure im Projekt nicht endlich beginnen, miteinander in den Dialog zu treten und im Vorfeld präventiv für geeignete Sicherheitsstrukturen durch Business Continuity Management zu sorgen, dann werden wir immer wieder Schlagzeilen über digitale Erpressung lesen – und dass das am Ende für Kliniken erst recht teuer und für Patient:innen lebensgefährlich wird, sollte allen klar sein.“

Literatur

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221025_Lagebericht.html

https://assets.sophos.com/X24WTUEQ/at/43hhrb4tjnjg8jj9fmjq6s/sophos-state-of-ransomware-2022-wpde.pdf