Die Medizin ist auf die schnelle Verfügbarkeit von Daten angewiesen. Und dabei oft auf sensible und sehr persönliche Informationen, die es zu schützen gilt. Umfassender und intelligenter Schutz sowie Verlässlichkeit sind dabei gefragt...

Ein Immunsystem fürs Krankenhaus

Es geht um den richtigen Abgleich zwischen Security und Safety", erklärt Robert Jankovics, IT-Sicherheitsexperte der Kapsch BusinessCom. *Security,* um die sensiblen Patientendaten vor unbefugten Personen zu schützen. *Safety,* um sicherzustellen, dass die behandelnden Ärzte jederzeit schnell und einfach Zugriff auf eben diese sensiblen Daten haben.

Dabei geht es um unterschiedliche Dimensionen der Datensicherheit im Gesundheitswesen. „Daten, gerade wenn es so persönliche Informationen wie den Gesundheitszustand von Menschen betrifft, genießen höchstes Schutzinteresse", erklärt Jankovics. Eigentlich eine Selbstverständlichkeit. In einem Umfeld, das in seinem Wesen auf den Austausch von Wissen, auf die schnelle Verfügbarkeit von Informationen setzt, wie eben einem Krankenhaus ist das allerdings nicht so leicht zu bewerkstelligen. „Was früher lediglich auf dem Papier vorhanden war – Details zu jedem einzelnen Patienten, zu seiner Medikation, zu seiner Krankengeschichte, zu seiner Vorgeschichte – all das ist heute digital erfasst und in einem zentralen Register gespeichert", umreißt der Fachmann den Ausgangspunkt.

Auf dieses Register und das darin gespeicherte Wissen müssen die Ärzte Zugriff haben. Sprich, es kann nicht hermetisch abgeschottet werden. Womit das Risiko steigt, dass Daten in unbefugte Hände geraten. „Man muss sich vor Augen halten, dass in einem Krankenhaus nicht allein ein einschlägiges Informationssystem vorhanden ist. Die Netzwerke umfassen viele unterschiedliche Komponenten – bis hin zur Haustechnik. Und über unterschiedlichste

Netzwerkzugänge können sie angesteuert werden, teilweise sogar über das Internet."

Diese Problematik sei bekannt, hält Jankovics fest. Manchen ist sie freilich in ihrer Tragweite nicht ganz bewusst. „Zunächst erheben wir den Ist-Stand. Das bedeutet: Klären, was gegeben ist und was gebraucht wird. Wir durchforsten das Gebäude und die Institution gleichermaßen." Man könnte auch sagen, Jankovics und sein Team führen eine umfassende Anamnese durch.

Ein „Kreislauf" verhilft zum „Immunsystem"

Aus IT-Sicht trifft eine Vielzahl von Aufgaben aufeinander: die Verwaltung und Lagerung von Medikamenten, die Zutrittskontrollen, die Haustechnik, die Wäsche, das Krankenhausbüffet uvm. Und alle hängen sie zusammen. Sei es nur dadurch, dass sie über ein und dasselbe Netz kommunizieren. Alle diese Dimensionen müssen erschlossen und in ihrer Bestandsaufnahme festgehalten, ihre Verbindungen ausreichend exakt dargestellt werden. Erst dann kann ein Sicherheitskonzept erstellt werden.

Ein Maßnahmenplan, der Schritt für Schritt erfolgt, der kein finales Datum kennt, stattdessen immer neue Erkenntnisse und Notwendigkeiten hervorbringt. Es wird ein Kreislauf in Gang gesetzt, der aus den vier Elementen „Prevent", „Protect", „Detect" und „Respond" besteht. Aus adäquaten, individuellen Lösungen unterschiedlicher Herausforderungen.

„Der erste Schritt ist eine Netzwerksegmentierung", erklärt Jankovics. Gibt es irgendwo im Netzwerk einen Zwischenfall, verhindert diese Segmentierung die Ausbreitung. Es schließen sich gleichsam die Schotten, sodass kein Durchkommen mehr gegeben ist. „Eine gesamtheitliche Maßnahme", so Jankovics, „die schnelle Verbesserung bringt." Sozusagen die Basisvariante der Sicherheit.

Für die Experten von Kapsch BusinessCom geht es in weiterer Folge immer tiefer in die einzelnen Teilbereiche, in denen es zunehmend komplexer wird. „Wir orientieren uns an den Fragen: Was sind die Hauptaufgabengebiete? Was sind die wichtigsten Kernprozesse? Wo und auf welchen Systemen finden sie statt?"

Nach und nach entsteht so eine personalisierte Sicherheitsstruktur für eine Gesundheitseinrichtung. Eine Struktur, die eigene Sicherheitszonen festschreibt und definiert. „Nehmen wir als einfaches Beispiel einen Chirurgen im Operationssaal. Der braucht Informationen von jetzt auf gleich. Der kann sich nicht damit aufhalten, dass er erst Passwörter eingeben soll." Also wird dieser OP als Ort definiert, von dem aus Anfragen zu bestimmten Themen ohne große Sicherheitsschleusen gestellt werden dürfen. „Dieselbe Anfrage aus der Pförtnerloge würde abgelehnt", skizziert Jankovics die Geographie unterschiedlich definierter Sicherheitszonen. Im Zuge dieser Maßnahmen werden lokal gebundene Freiräume geschaffen, die sich digital widerspiegeln.

Back-up schützt bei Hackerangriff

Doch das ist noch nicht alles. „Wir haben mit einem Spital eine Institution, die ununterbrochen Daten produziert. Informationen, die essenziell sind", spinnt Jankovics den Faden weiter. Nun gilt es, diesen steten Strom zu erfassen und zu sichern. Die Daten müssen in Echtzeit speicherbar sein. Dazu braucht es eine leistungsfähige und zuverlässige Back-up-Struktur.

Wichtig sind diese Back-ups nicht allein zur Archivierung. Sie sind die beste Versicherung gegen bestimmte Formen der Cyberkriminalität. Im Mai 2017 erbeuteten Hacker bei einem Angriff auf den britischen National Health Service (NHS) riesige Mengen an Patientendaten. Weltweit häufen sich Fälle, in denen Hacker Krankenhausdaten verschlüsseln und blockieren, um dann Lösegeld zu fordern. 2016 sorgten Ransomware-Attacken im deutschen Neuss dafür, dass ein Spital nach Cyber-Angriffen und Lösegeldforderungen Patienten abweisen musste. Bei Weitem nicht der einzige Vorfall dieser Art. „Wir wissen von Attacken, in denen die Krankenhäuser mithilfe ihrer Back-up-Struktur die verschlüsselten Daten zurückgewinnen konnten. Wir wissen aber auch von Fällen, in denen Lösegeld bezahlt wurde", schildert Jankovics.

Ausschließen kann man Angriffe nicht. Aber schon eine gute Netzwerksegmentierung im Zusammenspiel mit einem Monitoring der Datenströme kann Unregelmäßigkeiten entdecken, Alarm auslösen und erste Sicherungsmaßnahmen setzen. Jankovics vergleicht das mit der Funktionsweise des Immunsystems, das Viren erkennt und entsprechend reagiert: „Das ist ein laufender Prozess. Das System erkennt Muster. Es erkennt sie mit der Zeit immer besser. Es lernt dazu. Genauso lernen auch die Menschen dazu, denen die Analyse der festgestellten Anomalien obliegt."

Bewusstsein geschaffen

Forciert wird das Bewusstsein für die Notwendigkeit einer sicheren IT-Struktur durch das neue österreichische Netz- und Informationssystemsicherheitsgesetz (NISG) zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit. Vor zwei Jahren als Richtlinie der Europäischen Union erlassen, ist es mit 29.12.2018 auch in Österreich in Kraft getreten. „Im Rahmen dieses NIS-Gesetzes werden Betreiber wesentlicher Dienste in Österreich identifiziert und mittels Bescheides informiert", so Jankovics. Damit gehen Verpflichtungen einher. Vor allem jene, dass betroffene Einrichtungen für die Informationssicherheit geradestehen müssen. „Offen ist derzeit nur, wie viele Spitäler vom Innenministerium in die Pflicht genommen werden", meint Robert Jankovics. Mit dem richtigen Abgleich zwischen Security und Safety werden sich auf jeden Fall bald schon mehr Krankenhausmanager und Mediziner auseinandersetzen müssen. ::

Kontakt:
Dipl. Ing. Robert Jankovics
IT-Sicherheitsexperte
bei Kapsch BusinessCom AG
Impact@kapsch.net
www.kapsch.net