HZ212317 · ISSN 1868-5757 · www.datakontext.com August/September **4/2022**

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

Penetrationstests – wie es wirklich um die IT-Sicherheit steht

Götz Schartner und Tobias Kopf von 8com erklären, wie sich die Cyberresilienz im Unternehmen wirkungsvoll stärken lässt

SPECIAL
in Kooperation mit
ATZ – Automobiltechnische Zeitschrift:

IT-Sicherheit in der Automobilbranche

Welche besonderen Herausforderungen an die Cybersicherheit warten in der Automobilindustrie – und mit welchen Ansätzen werden sie erfolgreich gemeistert

SCHWERPUNKT

Penetrationstests:
Formen, strategische Einsatzbereiche und Ziele der „bezahlten Anriffe“

Entwicklung:
Quantensichere Kommunikation für hochsichere Netzwerke

Forschung:
Kennzahlen – wie Sicherheit im Internet messbar wird

DATAKONTEXT

Informationssicherheit kritischer Infrastrukturen im Gesundheitssektor

WIE KRITIS IHRE CYBER-SICHERHEIT STEMMEN

Sicherheit in der Informationstechnik – eine IT-Aufgabe? Das ist zu kurz gedacht. Der Schutz kritischer Infrastrukturen auch vor Cyberangriffen ist eine Managementaufgabe und setzt den Aufbau eines ISMS (Information Security Management System) voraus. Branchenspezifische Standards, Umsetzungshinweise und begleitendes Coaching durch externe Experten helfen bei der Lösung.

Cyberattacken bergen für alle Unternehmen hohe Risiken: Es drohen Produktionsausfälle, Datenverlust, Lösegelderpressung. Weit größer sind aber die möglichen Schäden bei Angriffen auf kritische Infrastrukturen, zu denen auch die Gesundheitsversorgung zählt. Denn Ausfälle in diesen Bereichen wirken sich nicht nur auf die einzelnen Unternehmen aus, sondern können die Grundversorgung oder die öffentliche Sicherheit gefährden. Betreiber kritischer Infrastrukturen sind daher per Gesetz zum besonderen Schutz ihrer informationstechnischen Systeme verpflichtet.

SICHERHEITSVORGABEN DURCH KRITIS UND KRITIS LIGHT

Im Gesundheitswesen gehören zu den kritischen Dienstleistungen die stationäre medizinische Versorgung sowie die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, verschreibungspflichtigen Arzneimitteln, Blut- und Plasmakonzentraten ebenso wie die Labordiagnostik. Die entsprechenden Anlagen gelten ab einer festgelegten Größe (Schwellenwert) als kritische Infrastrukturen. Die Betreiber müssen angemessene Vorkehrungen treffen, um Störungen der – für die Funktion der jeweiligen kritischen Infrastruktur maßgeblichen – informationstechnischen Systeme zu vermeiden. Diese Sicherheitsvorkehrungen sind gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) alle zwei Jahre nachzuweisen und an den Stand der Technik anzupassen (§ 8a BSI-Gesetz). Unabhängig von der Größe gelten die Verpflichtungen zur Informationssicherheit seit Januar 2022 für alle Krankenhäuser, lediglich die Nachweispflicht gegenüber dem BSI entfällt. Grundlage dieser oft auch als „KRITIS light" bezeichneten Vorgaben ist § 75c des Sozialgesetzbuches (SGB) V.

Insbesondere für kleinere Krankenhäuser, die neu mit dieser Herausforderung konfrontiert sind, stellt sich die nun die Frage, wie die IT-Sicherheitsvorgaben umzusetzen sind. Da es um den Schutz der Informationssysteme geht, scheint es naheliegend, die IT-Abteilung damit zu beauftragen. Doch dieser Ansatz greift zu kurz. Natürlich kommt der IT eine sehr wichtige Rolle bei der Erkennung und Bekämpfung von Cyberangriffen zu. Ziel der KRITIS-Verordnungen im Gesundheitssektor ist aber, durch angemessene technische und organisatorische Maßnahmen die Kernfunktionen aufrechtzuerhalten, also die Versorgung der Patienten wie auch die Datensicherheit zu gewährleisten.

WARUM DIE UMSETZUNG DER KRITIS-VORGABEN KEIN IT-PROJEKT IST

Inwieweit mögliche Störungen der IT-Strukturen tatsächlich auch die Kernfunktionen der betroffenen Infrastruktur beeinträchtigen, hängt vom Stand der Digitalisierung ab. Hier gibt es innerhalb des Gesundheitssektors beträchtliche Unterschiede. Während sich in den hochgradig automatisierten, produzierenden Bereichen der Pharmaindustrie IT-Ausfälle direkt auf die Kernprozesse wie die Arzneimittelproduktion auswirken, sind bei vergleichbaren Störungen in Krankenhäusern die medizinischen Prozes-

Bilder: Pixabay

se nicht zwingend gefährdet. Oft erleichtern hier IT-Prozesse die organisatorischen Abläufe; die Vorgänger-Prozesse wie schriftliche Aufzeichnungen, Vermerke oder Kennzeichnungen sind aber oft noch in der Organisation bekannt. Mitarbeitende können dann bei Störungen der IT sehr schnell auf solche früher geläufigen Vorgehensweisen zurückgreifen. Für technische Ausfälle während einer Operation sind ohnehin feste Prozesse etabliert wie etwa Stabilisierung der Patienten und Überwachung in der Intensivstation.

An dieser Stelle wird bereits deutlich, worin die eigentliche Herausforderung bei der Umsetzung der IT-Sicherheit nach KRITIS und KRITIS light besteht: in der Analyse, Bewertung und Überarbeitung aller relevanten Unternehmensprozesse. Nicht nur die Bewältigung einer Bedrohungssituation ist untrennbar verknüpft mit bestehenden Ersatzprozessen, insbesondere dem Notfall-Management, auch die Gefährdung selbst geht neben typischen Software-Schwachstellen eben auch von menschlichen Fehlern aus (Beispiel: Social Engineering). Unzureichend kontrollierte Zugangs- und Zutrittsbeschränkungen, fehlende Sicherheitsvorgaben schon bei der Beschaffung oder weitere Prozessmängel können ebenfalls eine Rolle spielen. Und auf viele dieser Prozesse haben IT-Verantwortliche gar keinen Einfluss.

INFORMATION-SECURITY-MANAGEMENT-SYSTEME UND DIE ROLLE DER GESCHÄFTSLEITUNG

Um KRITIS-Sicherheitsvorgaben im Health-Care-Sektor erfolgreich umsetzen zu können, brauchen Unternehmen daher zunächst ein Informationssicherheitsmanagementsystem (ISMS). In der Struktur und Funktionsweise ist das am ehesten mit einem Qualitätsmanagement-System vergleichbar. Wie Krankenhausbetreiber diese Aufgabe angehen können, dazu gibt die Deutsche Krankenhausgesellschaft sowohl durch die Definition eines branchenspezifischen Sicherheitsstandards als auch durch konkrete Umsetzungshinweise zum Aufbau eines ISMS, GAP-Analysen, Übersichten und Templates wertvolle Hilfestellung.

Ein Punkt ist dabei besonders wichtig: Der Aufbau eines ISMS und die Etablierung branchenspezifischer Sicherheitsstandards sind Managementaufgaben. Das heißt, die Initiative dazu muss von der Geschäftsführung ausgehen, ISMS-Beauftragte sollten bereichsübergreifend agieren können und direkt an die Geschäftsleitung berichten.

BEGLEITENDES COACHING UND KNOW-HOW-AUFBAU IM UNTERNEHMEN

Doch selbst mit Best Practices, Arbeitshilfen und der vollen Unterstützung durch die Geschäftsleitung ist die Umsetzung der IT-Sicherheitsvorgaben in den kritischen Infrastrukturen und Krankenhäusern komplex und herausfordernd. Die größte Hürde ist dabei der Personalmangel. Es braucht zumindest eine verantwortliche Person, um ein ISMS aufzubauen und zu betreuen. Experten für Cybersecurity aber sind rar; die sparsam besetzten, hauseigenen IT-Abteilungen in der Regel schon mit dem Tagesgeschäft völlig ausgelastet.

Gerade Einrichtungen, die noch kein ISMS etabliert haben, werden daher Unterstützung durch externe Spezialisten benötigen. Dabei – und das ist die gute Nachricht – steht aber gar kein großes und ressourcenbindendes Implementierungsprojekt an. In der Praxis hat sich ein stattdessen ein begleitendes Coaching-Modell bewährt. Berater und Projektverantwortliche im Unternehmen bilden dabei ein Tandem, indem sie sich in ihren Kompetenzen ergänzen: Berater kennen aus ihrer Projekterfahrung mehrere erfolgreiche Lösungsoptionen und stellen diese vor. Die intern verantwortliche Person kann aufgrund ihrer Betriebskenntnis beurteilen, welche dieser Optionen zum eigenen Unternehmen passt.

Daraus ergibt sich als grundlegende Anforderung bei der Auswahl geeigneter interner Kandidaten, dass diese mit den Abläufen im Unternehmen sehr gut vertraut und auch intern gut vernetzt sein müssen. Die spezifischen Skills für die Betreuung des ISMS dagegen können im Laufe der begleitenden Beratung erlernt werden. Die Intensität des Coachings ist dabei zu Beginn am höchsten und nimmt im weiteren Verlauf ab, da intern Verantwortliche zunehmend selbstständig agieren. Es findet also ein nachhaltiger Wissenstransfer statt, während Anfangsfehler vermieden werden.

INFORMATIONSSICHERHEIT IST EIN PROZESS

Dieses Know-how im Unternehmen aufzubauen ist auch deshalb wichtig, weil Informationssicherheit ist kein statischer Zustand ist, sondern ein fortlaufender Prozess. Eine Überprüfung und Anpassung an den Stand der Technik muss spätestens alle zwei Jahre erfolgen. Vor allem aber erhöhen sich im Zuge der Digitalisierung und der immer stärkeren Vernetzung auch die Komplexität und Vulnerabilität der Prozesse und Systeme. Die Maßnahmen zur Informationssicherheit sind also kontinuierlich anzupassen. ■

RANDOLF SKERKA,
Business Development Manager
Healthcare SRC Security Research
& Consulting