Frankfurter Rundschau; Samstag, 10.02.2024
„Dr. Hontschiks Diagnose“

Schöne neue Welt

Alarmierende Zunahme der Cyber-Attacken im Gesundheitswesen

Ein neues Wort ist in unseren täglichen Sprachgebrauch eingewandert: Es ist das Wort „Cyber“, das von Kybernetik abgeleitet und fast ausschließlich als Vorsilbe benutzt wird. Das Wort signalisiert, dass sich etwas im virtuellen Raum abspielt, dem Cyberspace. Aber Cyberkrieg, Cybersicherheit, Cybermobbing und Cyberkriminalität haben massive Konsequenzen in der Realität, inzwischen auch in unserem ganz realen Gesundheitswesen. Nach Einschätzung des Bundesamtes für Sicherheit und Informationstechnik ist die Bedrohungslage im Gesundheitswesen aktuell so hoch wie noch nie. Das zeigt eine kleine Auswahl des Grauens aus den letzten zwei Jahren: Februar 2024, Berlin; Nach einem Cyber-Angriff kam es zu einem kompletten Ausfall der IT-Systeme der Caritas-Klinik Dominikus in Berlin-Reinickendorf. Vom Wiederaufbau der IT-Struktur werden „Fortschritte“ gemeldet. Februar 2024, Nordrhein-Westfalen; Die Cyber-Attacke traf das Dreifaltigkeits-Hospital in Lippstadt und den Klinikverbund mit Häusern in Erwitte und Geseke. Eine stationäre Aufnahme von Notfällen war länger nicht möglich, sie mussten an benachbarte Krankenhäuser verwiesen werden. Februar 2024, Mittelfranken; Angegriffen wurde Krankenhäuser in Ansbach, Erlangen und Engelthal. Externe Fachleute suchen nach der Schwachstelle, andere sind dabei, das IT-System in den drei Krankenhäusern neu aufzusetzen. Dezember 2023, Esslingen; Auf das Klinikum Esslingen gelang der Angriff über den Citrix-Zugang, der Fernzugriffe möglich macht. Ein Krisenstab musste eingerichtet werden. Dezember 2023, Ostwestfalen; Am Weihnachtsabend sind die IT-Systeme von drei ostwestfälischen Krankenhäusern vollständig ausgefallen, beim Franziskus Hospital in Bielefeld, dem Sankt Vinzenz Hospital in Rheda-Wiedenbrück und dem Mathilden Hospital in Herford. Oktober 2023, Frankfurt am Main; Nach einem erfolgreichen Hacker-Angriff muss die Universitätsklinik die IT komplett neu aufstellen. Eine dreistellige Zahl an Fachleuten ist immer noch damit beschäftigt, die Cyberattacke aufzuarbeiten und Übergangslösungen zu bauen. Bis alles wieder ohne Einschränkungen läuft, „wird es Monate dauern“. Juni 2023, Bremen; Hacker kopierten bei einem Cyber-Angriff auf das Klinikum Bremen-Ost rund 700.000 Patientendateien. Der Krankenhausverbund befürchtet, dass diesmal versucht wird, betroffene Patient:innen zu erpressen. November 2022, Detmold; Nach einem massiven Cyber-Angriff auf das Klinikum Lippe ist die gesamte IT-Struktur des Krankenhauses an allen drei Standorten in Detmold, Lemgo und Bad Salzuflen von allen Netzen getrennt worden.

Auch Arztpraxen sind inzwischen betroffen. Schon im März 2022 berichtete ein Berliner Augenarzt, dass der Cyber-Angriff auf seine Arztpraxis erst nach der Zahlung eines erheblichen Lösegeldes beendet war. Cyber-Kriminelle hatten seinen Betrieb drei Wochen lahmgelegt.

Warum Krankenhäuser ein beliebtes Ziel von Cyberattacken sind, erklärt sich mit dem hohen Wert der gehackten Daten. Entweder werden die Patientendaten gestohlen und für viel Geld im Darknet weiterverkauft, oder es wird über sogenannte Trojaner eine Ransomware in die IT-Systeme eingeschmuggelt, womit alle Computer gesperrt sind. Die betroffene Klinik wird damit zur Zahlung von hohen Summen erpresst. In aller Regel wird gezahlt. Wer nicht zahlt, hat alles unwiederbringlich verloren.

Die zentrale Sammlung von hochsensiblen Informationen an einem einzigen Ort ist das eigentliche Problem. Kein zentraler Datenserver kann vor Hacker-Angriffen definitiv geschützt werden, ob es sich dabei um das US-amerikanische Verteidigungsministerium, den Deutsche Bundestag oder hochgerüstete Kreditkarten-Unternehmen handelt. Es empfiehlt sich daher zwingend eine dezentrale Verwaltung und Vernetzung von Patientenakten und allen anderen Gesundheitsdaten, etwa in Form von Netzwerken und dezentralen Zugriffsalgorithmen aus dem Bereich der Blockchain-Technologie.

Es ist unbegreiflich, und es sorgt nicht gerade für Vertrauen, wenn die geplante und für alle Bundesbürger:innen nahezu unentrinnbare elektronische Patientenakte, die vom Deutschen Bundestag soeben beschlossen worden ist, auf einer zentralen Servertechnologie aufgebaut wird. Tür und Tor weerden damit für Cyberkriminelle offen gehalten. Komplizierteste und für Benutzer:innen aufwändige und lästige Sicherungskonzepte werden Hacker-Zugriffe, Missbrauch, Datendiebstahl und Erpressung von Krankenhäusern, von Arztpraxen oder direkt von Patient:innen nicht verhindern können.

chirurg@hontschik.de www.medizinHuman.de