Cyberangriff auf die Gesundheit

Hacker haben schon bewiesen, dass vernetzte Medizinprodukte gegen Manipulationen von außen anfällig sein können. Doch Hersteller schließen die Sicherheitslücken oft nur langsam

Auch wenn das Herz des Patienten 355-mal schneller schlagen würde als normal, nämlich mit 32 000 Schlägen in der Minute anstelle von 90 – der Patientenmonitor am Krankenhausbett würde keinen Alarm schlagen. Er würde auch keine Warnung verschicken, wenn das Herz des Patienten einfach stehen bleiben würde. Der Patient würde sterben, die Technik hätte versagt.

Aber dieses Szenario wäre kein Unfall, sondern kaltblütiger Mord: Jemand hat den Monitor manipuliert, der die Werte des Patienten überwachen und das Klinikpersonal warnen soll, wenn die Werte in lebensbedrohliche Bereiche abdriften – und zwar aus der Ferne, ohne das Krankenzimmer überhaupt zu betreten. Er könnte in der Kantine gesessen haben, in einem Wartezimmer, sogar auf der Toilette.

Der Mann, der bewiesen hat, dass so ein Horrorszenario möglich wäre, heißt Florian Grunow – und er tat es mit den besten Absichten. Grunow ist kein Mediziner, sondern IT-Sicherheitsforscher der Firma ERNW. Er wählte sich in das Netzwerk eines Krankenhauses ein und übernahm von dort aus die Kontrolle über den Patientenmonitor, um zu zeigen, wie verheerend Hackerangriffe sein könnten, wenn sie sich gezielt gegen Krankenhäuser richteten. Die Klinik in Grunows Fall war vorher informiert, Menschen waren nicht in Gefahr.

In den USA gibt es pro Krankenbett zwischen zehn und 15 vernetzte Geräte, von Insulinpumpen bis hin zum Monitor, wie May Wang von der Cybersicherheitsfirma Zingbox erklärt. Jedes dieser Geräte ist an das Krankenhaus-Netzwerk angeschlossen oder erlaubt zum Beispiel Funkverbindungen, damit es aus der Ferne bedient werden kann. Dadurch ist es allerdings auch ein mögliches Angriffsziel.

Im August 2018 verschickte Abbott, ein Hersteller von Medizinprodukten, einen Brief, der Ärzte auf eine neue Version des Betriebssystems bei einem Herzschrittmacher hinwies. In der bisherigen Version seien Schwachstellen enthalten gewesen. Weltweit 745 000 Menschen mussten einen Termin mit ihrem Arzt ausmachen, damit dieser das Update einspielen konnte. Für Herzschrittmacher gibt es spezielle Kontrollgeräte, über die zum Beispiel die Batteriespannung geprüft werden kann. Dazu wird ein Programmierkopf auf die Haut des Patienten gelegt, so werden die Daten ausgelesen – und so werden auch Updates eingespielt.

Vernetzte Geräte in Krankenhäusern bieten den Luxus, dass sie aus der Ferne überwacht werden können. Das macht sie aber auch angreifbar. FOTO: MAURITIUS-IMAGES

Die Bundesregierung sieht in der Digitalisierung „eine der größten Herausforderungen des Gesundheitswesens in den nächsten Jahren". Dazu gehören elektronische Gesundheitsakten, Krankenhäuser, in denen Ärzte sich alle Informationen auf Tablets anschauen können, sowie medizinische Geräte mit Update-Funktion. Ärzte erhoffen sich davon eine bessere Behandlung und mehr Effektivität. Das Lukaskrankenhaus in Neuss teilte dem Magazin *Stern* zum Beispiel mit, dass dank Telemedizin die Sterblichkeit nach Herzinfarkten um 23 Prozent gesunken sei.

Zwei Drittel aller deutschen Kliniken waren bereits Cyberangriffen ausgesetzt

Was die Medizin modernisieren soll, kann sie gleichzeitig für Angriffe öffnen, sagt Grunow: „Die meisten Hersteller von medizinischen Geräten haben IT-Sicherheit erst seit zwei Jahren auf dem Ticker." Und auch bei Kliniken sieht es ähnlich düster aus: Nach einer Studie des Beratungsunternehmens Roland Berger waren zwei Drittel aller deutschen Kliniken bereits Opfer von Cyberangriffen.

Erst langsam würden Verantwortliche merken, dass alte Regeln außer Kraft gesetzt seien. „Man ging bis vor Kurzem davon aus, dass die Geräte in einem abgeschlossenen Bereich aufgestellt werden,

Süddeutsche Zeitung, Implant Files, S.11, 30.11.2018

an den Unbefugte nicht so einfach rankommen", sagt Grunow, dem es vergangenes Jahr sogar gelungen ist, ein Narkosegerät zu hacken: „Solche Geräte stellen die Beatmung des Menschen sicher, auch dann, wenn die Software abstürzt. Wir haben das Gerät komplett ausschalten können." Menschen waren auch hier nicht in Gefahr, die Klinik war informiert. Über das Netzwerk sei es möglich gewesen, auf den Apparat zuzugreifen. Im Ernstfall wäre die Beatmung durch einen Hacker gestoppt worden.

Grunow wies die Hersteller auf die Schwachstelle hin. Doch anstatt sich zu bedanken, drohten diese dem IT-Experten per Anwalt mit rechtlichen Konsequenzen. Um die Geräte auszuschalten, so wie Grunow das schildert, müssten die Hacker sich allerdings im Netzwerk des Krankenhauses befinden, zum Beispiel im WLAN. Ein gezielter Angriff aus dem Internet gegen eine Einzelperson wird von Experten wie Grunow daher als eher unwahrscheinlich eingeschätzt. Derzeit gibt es keine Angriffe, bei denen sich etwa Herzschrittmacher aus der Ferne hacken lassen – wie das zum Beispiel in der US-Serie *Homeland* passiert. Dort stirbt der US-Vizepräsident durch genau solch eine Tat.

Sind die Geräte richtig konfiguriert, kann man nicht aus dem Internet auf sie zugreifen, um zum Beispiel Patientendaten auszulesen. Doch auch hier unterlaufen Krankenhäusern Fehler. Wie Experten der IT-Sicherheitsfirma Trend Micro herausfanden, lassen sich über eine spezielle Suchmaschine weltweit mehr als 100 000 medizinische Geräte finden, die direkt an das Internet angeschlossen sind. Das heißt zwar nicht, dass all diese Geräte angreifbar sind, erklärt Udo Schneider, IT-Sicherheitsexperte bei Trend Micro – aber Hacker könnten bei diesen Geräten durchaus anfangen, nach Schwachstellen zu suchen. „Bei medizinischen Geräten werden meist die Standard-Passwörter nicht geändert", sagt Schneider. Hinzu komme, dass die Zertifizierung der Geräte erlösche, wenn man sie nach Inbetriebnahme mit neuer Software aktualisiere. „Dann müsste das Gerät neu abgenommen werden. In der Realität sieht es deshalb so aus, dass die Software meist veraltet ist", sagt Schneider. Die Hersteller scheuten seiner Ansicht nach die Bürokratie mit den Zertifizierungsstellen und würden die Updates daher bisweilen nur mit Verzögerung bereitstellen. Hacker könnten deshalb Sicherheitslücken ausnutzen, auch wenn diese schon vor Jahren geschlossen worden seien. Denn die Systeme werden nicht aktualisiert. Für Hacker sind diese Geräte daher ein potenzielles Ziel.

HAKAN TANRIVERDI

Wenn Sie Fragen zum Thema Implantate oder Medizinprodukte haben, können Sie sich bei Ihrem Arzt melden oder bei der SZ. Das Team der Implant Files erreichen Sie unter implant-files@sz.de. Alle bisher veröffentlichten Texte zum Thema finden Sie außerdem auf www.implantfiles.de.