Die offenen Wunden im System

Immer öfter werden Einrichtungen des Gesundheitswesens zum Ziel von Hackerangriffen. Anfällig für Attacken sind dabei nicht nur die Netzwerke, sondern auch die medizinischen Geräte.

AM FRÜHEN MORGEN des 10. Septembers 2020 dringen Hacker in das IT-System der Uniklinik Düsseldorf ein und verschlüsseln dort den Zugang zu 30 Servern. Die Täter nutzen dabei die Schwachstelle in einer marktüblichen und kommerziell verbreiteten Zusatzsoftware aus. Mehr als eine Woche lang ist die digitale Infrastruktur des Krankenhauses weitgehend lahmgelegt. Aus Sicherheitsgründen müssen Operationen verschoben, und auch die Notfallaufnahme muss geschlossen werden, weil Mitarbeiter nicht mehr auf das Computerprogramm zugreifen können. Sensible Patientendaten wie Befunde, Laborwerte und Röntgenbilder sind wie eingefroren. Keine Hubschrauber dürfen landen, keine Notarztwagen das Krankenhaus ansteuern. Eine schwer erkrankte Patientin, die im Rettungswagen um ihr Leben kämpft, wird deshalb an der Uniklinik abgewiesen. Der Rettungsdienst fährt weiter nach Wuppertal. Mehr als eine halbe Stunde geht so verloren. Kurz nach ihrer Ankunft im Krankenhaus stirbt die Frau. Die Staatsanwaltschaft ermittelt wegen des Verdachts auf fahrlässige Tötung.

Sicherheitsprobleme waren bekannt

Wie sich anhand der Obduktion herausstellt, wäre die Frau wahrscheinlich auch gestorben, wenn die Düsseldorfer Klinik sie aufgenommen hätte. Die Ermittlungen wegen fahrlässiger Tötung werden eingestellt, die Suche nach den Hackern geht weiter. Auf einem der Server wird ein Erpresserschreiben hinterlassen, das allerdings nicht an die Uniklinik, sondern an die Düsseldorfer Heinrich-Heine-Universität gerichtet ist. Als den Tätern womöglich bewusst wird, dass ihr Angriff Menschenleben gefährdet, händigen sie den digitalen Schlüssel für den Server aus. Allem Anschein nach wurden weder Daten gestohlen noch unwiderruflich gelöscht. Es hätte also schlimmer kommen können. Und es hätte vor allem vermieden werden können. So hatte das Bundesamt für Sicherheit (BSI), das unter anderem für den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge zuständig ist, nach eigenen Angaben bereits Monate zuvor vor Sicherheitsproblemen der Software gewarnt. Die Softwarefirma hatte darauf auch bereits reagiert, nur waren die Hacker allem Anschein nach schneller. Sie nutzten das kurze Zeitfenster, um in das System der Uniklinik einzudringen.

Menschliche Schwachstelle im System

Eingesetzte Komponenten müssen zertifiziert sein

Die Cyberattacke auf die Düsseldorfer Uniklinik ist bei weitem kein Einzelfall. Laut Bundesregierung ist die Zahl der Angriffe im Gesundheitsbereich in den vergangenen Jahren drastisch gestiegen. Wurden 2018 noch elf und im Jahr darauf 16 Fälle erfasst, waren es im vergangenen Jahr allein im Zeitraum Januar bis Mitte November 43.

Die Zahl der Angriffe steigt

Betroffen davon sind vor allem Krankenhäuser. Sie gehören zu den Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Allgemeinwesen und sind Teil der Kritischen Infrastrukturen (KRITIS), deren besonderer Schutz über das sogenannte IT-Sicherheitsgesetz geregelt ist. Ende 2020 hat das Bundeskabinett einen Entwurf für das IT-Sicherheitsgesetz 2.0 gebilligt. Mit diesem werden die Befugnisse des BSI zum Schutz kritischer Systeme erweitert und der Verbraucherschutz gestärkt. Das BSI soll nun auch Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen und Medienangeboten unterstützen. Zudem dürfen KRITIS-Einrichtungen in ihrer IT nur noch Komponenten einsetzen, die über ein BSI-Sicherheitskennzeichen verfügen. »Wir haben in den letzten Jahren viel gegen den Terror getan. Wir müssen genauso viel dafür tun, dass Hacker und Spione nicht die Schaltzentralen unserer Krankenhäuser oder Energieversorger kapern«, rechtfertigt Innenminister Horst Seehofer den Entwurf des Gesetzes. Es sei ein »Durchbruch für Deutschlands Cybersicherheit«.

Schnittstellen werden zu Schwachstellen

Fast am gleichen Tag hat das Bundesamt für Sicherheit den Abschlussbericht des Projekts *ManiMed* (Manipulation von Medizinprodukten) vorgelegt. Das BSI-Projekt hat sich mit der Cybersicherheit vernetzter Medizinprodukte befasst.

Untersucht auf ihre Anfälligkeit wurden dabei Herzschrittmacher, Insulin- und Infusionspumpen, Beatmungsgeräte und Patientenmonitore. Elf Geräte mit Netzwerk- und Kommunikationsschnittstellen wurden überprüft, mehr als 150 Schwachstellen wurden dabei definiert. Wie aus dem Bericht hervorgeht, waren die Schwachstellen häufig nicht in den Medizinprodukten selbst, sondern vermehrt in der ergänzenden Infrastruktur zu finden. Die Infusionspumpen beispielsweise erwiesen sich als äußert robust und selbst bei einem Infrastrukturausfall als zuverlässig, wohingegen die Dockingstationen der Pumpen aufgrund ihrer Kommunikationsschnittstellen eine Angriffsfläche boten. Die Hersteller der medizinischen Produkte wurden im Rahmen der Überprüfung auf die Schwachstellen hingewiesen und diese dann auch sehr schnell beseitigt. Wichtig sei, entdeckte Mängel offen zu kommunizieren, rät die für den ManiMed-Report zuständige BSI-Referentin Dina Trixius betroffenen Unternehmen und Einrichtungen. »Es ist keine Schande, wenn Schwachstellen in Produkten entdeckt werden«, so Trixius.

Ein kleiner Klick mit großer Wirkung

Eine wesentliche Schwachstelle im System ist und bleibt der Mensch. Ein Klick auf den manipulierten Link in einer E-Mail löst die Kettenreaktion aus. Und die Zahl der Schadprogramm-Varianten, die diese Schwäche ausnutzen, wächst rasant. Laut BSI sind allein im Zeitraum Juni 2019 bis Mai 2020 mehr als 117 Millionen neue Schadsoftware-Varianten aufgetaucht. Als eine der größten Bedrohungen für kritische Infrastrukturen gilt die *Ransomware*. *Ransom* ist das englische Wort für Lösegeld, und genau darum geht es. Der erfolgreiche Einsatz dieser Art von Schadsoftware verhindert den Zugriff auf lokale oder im Netzwerk erreichbare Daten und Systeme. Oft werden Nutzerdaten oder ganze Datenbanken verschlüsselt. Die Opfer erhalten anschließend eine Nachricht, dass die Beschränkung bei Zahlung eines Lösegelds wieder aufgehoben werde. Gedroht wird dabei in der Regel mit einer sukzessiven Löschung oder Veröffentlichung der verschlüsselten Daten.

Erfolgreicher Schlag gegen gefürchteten Trojaner

Der mit Abstand bekannteste Vertreter der Ransomware ist das Schadprogramm *Emotet*. Vor zwei Jahren wurde das Klinikum Fürth Opfer eines Hackerangriffs, bei dem ebenfalls der gefürchtete Trojaner zum Einsatz kam. Genau wie in Düsseldorf wurde der Krankenhausbetrieb weitgehend lahmgelegt. Eingeschleust wurde das Virus nach Angaben der Klinik per Mail. Wie viel Schaden Emotet bislang weltweit angerichtet hat, lässt sich kaum beziffern. Das Bundeskriminalamt geht aber davon aus, dass der Trojaner, dessen Netzwerk Anfang des Jahres durch eine gemeinsame Aktion von Europol und Eurojust zerschlagen wurde, allein in Deutschland seit 2018 einen Schaden von 14,5 Millionen Euro verursacht hat.

Corona lässt grüßen

Es gibt aber auch noch ein weiteres Virus, das die IT-Sicherheit von Krankenhäusern gefährdet. Und das ist COVID-19. Seit dem Ausbruch der Pandemie haben die Cyberattacken spürbar zugenommen. Experten vermuten, dass die Hacker die prekäre Situation der Krankenhäuser gezielt ausnutzen. »Die Corona-Pandemie hat gezeigt, dass die Digitalisierung in Krankenhäusern noch nicht im notwendigen Maß entwickelt ist und genutzt wird«, so Gerald Gaß, Präsident der Deutschen Krankenhaus-Gesellschaft (DKG), der in dem vom Bundestag im Herbst 2020 verabschiedeten *Krankenhauszukunftsgesetz* einen deutlichen Schub für die Digitalisierung der Krankenhäuser sieht. Das Gesetz sieht vor, dass von den darin vorgesehenen 4,3 Milliarden Euro aus Bundes- und Landesmitteln mindestens 15% in die IT-Sicherheit investiert werden müssen. Das Corona-Virus hat also ungewollt auch die Entwicklung in die gewünschte Richtung beschleunigt. Wären da nur nicht die vielen anderen Viren, die nach jeder Sicherheitslücke im System Ausschau halten.

Mehr Cyberattacken seit Corona

Uwe Hentschel lebt und arbeitet als freier Journalist in der Eifel und schreibt dort für deutsche und luxemburgische Medien.
hentschel@geeifelt.de