Wenn Spitäler Opfer von Cyberattacken werden

Demonstrationslabor für Medizintechnik erforscht Schwachstellen der Cybersecurity im Gesundheitswesen

Robert Prazak

Wien – Diebstahl von heiklen Daten über den Gesundheitszustand einer Person. Medizingeräte, die nach einem Hacker-Angriff plötzlich spinnen. Krankenhäuser, die nach der Installation eines Schadprogramms Lösegeld bezahlen müssen, damit die IT-Systeme wieder einwandfrei funktionieren. Cybersecurity ist im Gesundheitswesen derzeit ein großes Thema, denn mit der zunehmenden Vernetzung der Geräte und der steigenden Verwendung mobiler Applikationen steigt die Gefahr, dass wissentlich oder unwissentlich grobe Schäden angerichtet werden können.

In den USA kam es zuletzt zu sogenannten Ransomware-Attacken auf Spitäler. Dabei werden IT-Systeme durch Schadprogramme gesperrt und erst nach Zahlung eines Lösegelds („Ransom") wieder freigegeben. Zudem musste ein Hersteller von Insulinpumpen eine Schwachstelle in seiner Software zugeben: Hacker könnten die lebenswichtige Verwendung blockieren.

Georg Schnizer, Leiter der Abteilung Technologie und Informatik des Allgemeinen Krankenhauses Wien (AKH), konstatiert steigende Gefahr für Spitäler: „Durch die zunehmende Durchdringung mit IT, dem Aufkommen des Internet of Things und der steigenden Anzahl an Services erhöht sich die verfügbare Angriffsfläche, daraus resultiert auch eine Zunahme der Angriffe."

An der Fachhochschule Technikum Wien wird vor diesem Hintergrund nun ein Test- und Demonstrationslabor für Medizintechnik und eHealth eingerichtet, in dem sichere und einfach bedienbare Lösungen entwickelt werden sollen. Alexander Mense, Studiengangsleiter Informationsmanagement und Computersicherheit der Fachhochschule Technikum sagt dazu: „Wir verfolgen zwei Ziele: Erstens bieten wir Bausteine an und erstellen Guidelines für interoperable Anwendungen, die auch sicher sind. Zweitens zeigen wir vor, wie sichere Anwendungen funktionieren können."

In diesem „Innovation Lab" soll auf Basis von Open-Source-Komponenten gezeigt werden, wie Interoperabilität und Sicherheit in der Praxis umgesetzt werden können, beispielsweise bei den sogenannten mHealth-Apps. Denn Sicherheit im Gesundheitswesen betrifft keineswegs nur Krankenhäuser und Ärzte, sondern wegen der zunehmenden Verbreitung vernetzter Geräte für den Heimbedarf und Gesundheits-Apps so gut wie jeden von uns. „Da geht es auch um persönliche Daten, die an unterschiedlichste – oft für den Benutzer nicht ersichtliche – Server geschickt werden", sagt Mense.

Spitäler wie das Wiener AKH stellen sich Sicherheitsrisiken.

Foto: Corn

Chancen der Vernetzung

Die Möglichkeiten, die die Vernetzung bieten, sind auch positiv: Wenn etwa aktuelle Wetter- und Umweltdaten mit Daten über die eigene Gesundheit – etwa Blutdruck – kombiniert werden, kann das sinnvolle Anwendungen ergeben. In diesem Zusammenhang ist eine Einbindung von Open Data von Bedeutung, also der Zugang zu frei verfügbaren Daten. All das müsste aber jeweils auch unter dem Aspekt der Sicherheit betrachtet werden, warnt Mense. „Security ist oft kein Thema, weil es vielfach als zu kompliziert empfunden wird." Durch schlecht implementierte Sicherheitsmaßnahmen sei aber beispielsweise ein Eindringen in Apps sehr einfach.

Im Innovation Lab soll nun den App-Herstellern gezeigt werden, was getan werden muss und kann. Eine Rolle spielt dabei auch die Einstellung der einzelnen Person zur Sicherheit – ein Faktor, der beim Umgang mit privaten Daten derzeit unterschätzt wird.

Im Krankenhaus oder bei den Herstellern von Medizintechnik-Geräten geht es nicht um die Einstellung, sondern eher um die Kosten. „Sicherheit ist technisch möglich, aber natürlich auch eine Frage des Aufwands", sagt Mense.

Dabei sei aber technische Sicherheit alleine oft nicht ausreichend, denn es brauche auch organisatorische Maßnahmen wie Schulungen der Mitarbeiter. Im AKH werde die IT-Sicherheit unter anderem durch Weiterbildung der zuständigen Administratoren, Beobachtung der aktuellen Situation und durch interne sowie externe Tests gewährleistet, erläutert IT-Chef Georg Schnizer. Die Bedeutung sicherer Systeme sei den Krankenhäusern in Österreich bewusst, meint Mense.

Eine Rolle spielt aber auch die lange Lebensdauer medizinischer Geräte wie CT-Scanner – auf diesen sind teilweise alte Windows-Systeme im Einsatz, die gar nicht am neuesten Stand sein können und somit etwa für Malware anfällig sind. Das bestätigt Georg Schnizer: „Durch die langfristigen Zertifizierungen der Medizintechnikgeräte kommen teilweise ältere Systeme zum Einsatz."

Aus Sicht der IT wäre eine Änderung in den Zertifizierungsprozessen gut, um das Sicherheitsbewusstsein bei vernetzten und integrierten Systemen bei den Herstellern zu stärken. Die IT-Abteilung sollte bereits bei Beschaffung einbezogen werden oder kann dann durch spezielle Firewalls der Bedrohung entgegenwirken.