Eingebaute Sicherheit

Interview mit Jörg Kirsten, Dedalus HealthCare

Universitätsklinikum Frankfurt, Caritas-Klinik Dominikus in Berlin-Reinickendorf, Bezirkskliniken Mittelfranken, Dreifaltigkeits-Hospital in Lippstadt, Krankenhaus Lindenbrunn in Coppenbrügge – das sind nur die letzten einer ganzen Reihe von Gesundheitseinrichtungen, die jüngst Ziel krimineller Cyberangriffe wurden. Wie kann ein Softwareanbieter seine Kunden dabei unterstützen, sich vor derartigen Gefahren zu schützen? Das erläutert Jörg Kirsten, Group Chief Information Security Officer bei Dedalus HealthCare, im Interview.

Herr Kirsten, was tut Dedalus HealthCare, um seine Software fit gegen Cyberangriffe zu machen?

Jörg Kirsten: Wir prüfen vom Start des Entwicklungsprozesses jede Anforderung an neue Entwicklungen und Änderungen am System schon zum Definitionszeitpunkt im Rahmen der notwendigen Sicherheitsmaßnahmen, um eine sichere Softwareentwicklung zu gewährleisten.

Was heißt das?

J. Kirsten: Es geht um zwei Aspekte: Security by Design und Privacy by Design. Von Security by Design spricht man, wenn bei der Entwicklung von Hard- oder Software bereits von Anfang an darauf geachtet wird, Systeme möglichst ohne Schwachstellen und so robust wie möglich gegen Angriffe zu konzipieren. Die Sicherheit wird also bereits im Entwicklungsprozess berücksichtigt und in den kompletten Lebenszyklus eines Produkts integriert. Zu den Designkriterien zählen beispielsweise die Minimierung der Angriffsfläche, der Einsatz von Verschlüsselung und Authentifizierung sowie die Isolation sicherheitsrelevanter Bereiche. Hinter Privacy by Design verbirgt sich der Datenschutz durch Technikgestaltung, dass der Datenschutz also bei Datenverarbeitungsvorgängen am besten eingehalten wird, wenn er bei deren Erarbeitung bereits technisch integriert ist.

Wie muss ich mir den Prozess vorstellen?

J. Kirsten: Unsere Experten sind in den kompletten Prozess der Softwareentwicklung eingebunden, von der Erstellung der Anforderungen sowie der Definition, was zu tun ist, über die Projektdefinition für ein neues Release und die Behandlung von Störungen oder Defekten zur kontinuierlichen Prüfung bezüglich Schwachstellen in der Software. Die

manuelle Prüfung des Codes erfolgt durch das Vier-Augen-Prinzip; eingebundene Open-Source- und Java-Bibliotheken werden automatisch geprüft. Während der Validierung und Verifikation des Produkts nehmen wir einen vollumfänglichen Antiviren- und Antimalware-Scan über die gesamte Software vor, um sicherzustellen, dass das auszuliefernde Produkt frei von jeglichem Schadcode ist.

Welche Rolle spielen Advanced Managed Services in diesem Kontext?

J. Kirsten: Das ist ganz unterschiedlich, je nachdem, welches Servicemodell der Kunde gewählt hat. Beim Updateservice installieren wir die Updates für die Software und die Datenbank auf den jeweiligen Servern. Ebenfalls können wir beim Betrieb der Hardwarekomponenten, des Betriebssystems und der installierten Software durch Patchmanagement unterstützen. Gerade das ist ein wichtiger Beitrag zur Cybersecurity. Ein weiterer Service ist der Schutz vor maliziöser Software, also Antiviren-, Antimalware- und Antiransomware-Scanner, die auf den Maschinen implementiert werden. Mit einer im Hause weiterentwickelten Monitoringlösung überwachen wir kontinuierlich alle Systemparameter, so dass wir drohende Systemausfälle frühzeitig entdecken und proaktiv eingreifen können. Das sorgt für die Sicherstellung der Systemverfügbarkeit. Zusätzlich bieten wir seit kurzem zusammen mit unserem Partner, der r-tec IT-Security GmbH, ein umfangreiches Portfolio im Bereich IT-Security an.

Die Nachfrage nach Cloud-Lösungen steigt stetig. Wie gehen Sie damit um?

J. Kirsten: Wir gehen den Weg mit im Markt etablierten Partnern, die jahrelang bewährte Cloudinfrastrukturen – auch in anderen sicherheitssensiblen Branchen – bereitstellen. Wir sprechen hier vorrangig von Amazon Web Services, kurz AWS. Der Anbieter weist aktuell rund 150 Zertifikate und Testierungen aller Art nach. Damit sind wirklich alle Anforderungen in punkto Cybersicherheit seitens des Herstellers und des Lieferanten abgedeckt.
Das beinhaltet selbstverständlich auch aktuelle Anforderungen, etwa die nach dem Gesetz zur Beschleunigung der Digitalisierung im Gesundheitswesen. Es schreibt für Cloudlösungen ein weiteres Testat vor, das C5-Testat. Dabei handelt es sich um einen Standard des Bundesamts für Sicherheit in der Informationstechnik für Clouddienste, der die Anbieter zu strikten Sicherheitsanforderungen für die Umgebung verpflichtet, etwa Services wie SOC und SIEM. Jeder Gesundheitseinrichtung, die mit uns den Weg in die Cloud geht, garantieren wir, dass alle notwendigen Maßnahmen zur IT-Sicherheit adäquat umgesetzt sind.

Was bekommt der Kunde konkret von Dedalus HealthCare, wenn es um die Daten- und Systemsicherheit geht?

J. Kirsten: Sowohl AMS- als auch Cloud-Kunden unterstützen wir in diesen Bereichen und übernehmen je nach Systemumgebung in großen Teilen die Aufgaben bzgl. IT-Security. Die Basis dafür ist ein kontinuierliches Monitoring. Unsere Sicherheitssysteme senden unverzüglich einen Alarm, sobald eine Schadsoftware identifiziert oder eine Anwendung geblockt wurde. Damit ist die Gefahr vorerst abgewehrt. Es gibt aber auch Software, die nicht unmittelbar geblockt, sondern lediglich isoliert wird, weil nicht klar ist, ob sie eine Bedrohung darstellt. Da reagieren wir sofort, schauen uns die potenzielle Gefahr genauer an und entscheiden dann im Einzelfall, was zu tun ist. Deswegen ist es immens wichtig, dass rund um die Uhr Personen zur Verfügung stehen, die sich dieser Aufgabe sofort annehmen. Nicht jede dem System fremde Software ist bösartig. So können auch durch ein Update eine neue Funktion implementiert oder neue Katalogeinträge vorgenommen werden. Diese sind wichtig, und falls sie automatisch geblockt werden, kann das gegebenenfalls zum Ausfall einzelner Funktionen oder im schlimmsten Fall des gesamten Systems führen. Deshalb ist eine sofortige Kontrolle unerlässlich. Im Servicekatalog ist das ein optionaler Service, den das Krankenhaus bei uns zubuchen kann. Bei der Cloud ist er inklusive.

Vielen Dank für die hilfreichen Ausführungen, Herr Kirsten.

Interview: Ralf Buchholz