carmasec

security. done. right.

Digitale Krankheitserreger & Prävention – Impfen Sie sich gegen Cyber-Bedrohungen

Carsten Marmulla

April 2019

Zusammenfassung

Die digitale Transformation erfasst das Gesundheitswesen und ermöglicht neue Geschäftsmodelle, bessere Prävention vor Krankheiten, schnellere Anamnese sowie effizientere Betreuung von Patienten. Durch den zunehmenden Technologieeinsatz steigt allerdings auch das Risiko Opfer von Datendieben und Saboteuren zu werden. Professionelle Vorsorge und bewusster Umgang mit kritischen Daten und IT-Systemen schützen Sie vor diesen Risiken.

Schlagwörter

Cybersicherheit, Datenschutz, Risikomanagement, Technologiefolgenabschätzung, Datensouveränität

Einleitung

Wir befinden uns mitten in einem gesellschaftspolitischen Wandel. Die „digitale Transformation“ erfasst zunehmend mehr Branchen, verändert bestehende Geschäftsmodelle und -prozesse und erfordert von allen Betroffenen sowie Beteiligten sowohl die Fähigkeit als auch den Willen zur Veränderung und Innovation.

Forciert wird die Digitalisierung dabei von einer rasanten technologischen Entwicklung, die neue datengetriebene Geschäftsmodelle erst ermöglicht. Gerade das Gesundheitswesen hat große Chancen, da erstmals die Möglichkeit besteht, umfassende Patientendaten zu erfassen, zu speichern und zu analysieren – und dies bereits im Rahmen einer Überwachung des eigenen Gesundheitszustandes beispielsweise durch kontinuierliche Messung von Puls, Blutdruck oder Blutzuckerwerten.

Allerdings erhöht der weitreichende Einsatz von Technologien im Gesundheitswesen auch die Wahrscheinlichkeit von Sicherheitslücken und Angriffen auf IT-Systemen betroffen zu sein. Dabei ist festzustellen, dass selbst bei unverhältnismäßig hohem Aufwand für Qualitätssicherung kein absolut sicheres System entstehen kann. Die stetig steigende Komplexität erhöht zusätzlich das Risiko von ausnutzbaren Schwachstellen in Soft- und Hardware.

Bedrohungslage

Die verarbeiteten Gesundheits- und Patientendaten gelten im Regelfall als so genannte personenbezogene Daten besonderer Art, für die aufgrund Ihrer hohen Schutzbedürftigkeit in Bezug auf die Schutzziele Vertraulichkeit und Integrität strenge regulatorische und gesetzliche Vorgaben gelten. Der Zugriff, die Übertragung, die Verarbeitung und die Speicherung muss daher im Einklang mit datenschutzrechtlichen Anforderungen stehen. Neben allen gesetzlichen Vorgaben muss das Verständnis hinsichtlich der Kritikalität von Gesundheitsdaten vorhanden sein, eine missbräuchliche Veröffentlichung dieser Daten kann für Betroffene fatale Auswirkungen haben.

Für einen Angreifer sind diese Daten nicht nur wegen der streng vertraulichen Klassifizierung besonders wertvoll, sondern auch aufgrund der verfügbaren Datenvolumina; längst ist es mit überschaubarem finanziellem und technischem Einsatz nicht nur möglich dauerhaft Gesundheitsdaten zu erfassen, sondern auch große Datenmengen unbegrenzt zu speichern und für zukünftige Analysezwecke vorzuhalten.

Im letzten Jahrzehnt hat sich die Bedrohungslage außerdem drastisch verschärft, heutzutage gehen die gefährlichsten Angriffe von professionell organisierten – meist aus wirtschaftskriminellen Motiven getriebenen – Gruppen aus. Der klassische aus Geltungsdrang agierende Einzeltäter ist dagegen heutzutage keine ernstzunehmende Gefahr, da hierfür eine Vielzahl von Gegenmaßnahmen erprobt und im Einsatz sind. Bei professionellen Angreifern bleibt die große Herausforderung allerdings, deren Aktivitäten frühzeitig zu erkennen und anschließend wirksame Gegenmaßnahmen einzuleiten.

Chancen und Risiken

Einhergehend mit der Digitalisierung werden immer mehr technische Geräte über zumeist öffentliche Netze miteinander vernetzt. Fatalerweise sind nicht alle Geräte, die dies technische ermöglichen auch dazu geeignet auf diesem Wege kritische Daten miteinander auszutauschen, da technische Grundvoraussetzung zur gegenseitigen Authentifizierung oder auch Maßnahmen zur Datenverschlüsselung nicht vorgesehen sind und oftmals auch mit vertretbarem Zusatzaufwand nicht nachrüstbar sind.

Doch weitaus nicht alle Maßnahmen beziehen sich auf den Einsatz von Technologie. Bei einer Vielzahl der erfolgreichen Angriffe werden menschliche und organisatorische Schwachstellen ausgenutzt, sei es beim so genannten „Phishing“ oder anderen Ansätzen, die unsere Angewohnheiten ausnutzen, um Fehlverhalten zu provozieren. Mit relativ einfachen Mitteln – beispielsweise mit regelmäßigen Mitarbeiterschulungen zur Erhöhung des Bewusstseins für die Bedrohungslage und zur Kenntnis über gängige Angriffsvektoren und Vorgehensweisen – lässt sich das Risiko signifikant senken.

Im Gegensatz dazu dienen technische Maßnahmen wie der Schutz vor Schadsoftware („Virenscanner“) oder der Einsatz von Netzwerkfiltern („Firewalls“) dazu, einen notwendigen aber nicht hinreichenden Basisschutz aufzubauen. Wesentlicher ist es, auf technischer Ebene die verwendeten IT-Komponenten mit aktueller Software einzusetzen, um diese damit gegen bekannte digitale Krankheitserreger zu impfen. Gäbe es in diesem Kontext nicht auch noch unbekannte Schwachstellen (oftmals auch als „Zero-Day“ beschrieben), so ließe sich damit ein recht effizienter und wirkungsvoller Schutz aufbauen.

Zu berücksichtigen ist ferner, dass es keineswegs notwendig oder erforderlich ist, überall eine generelle Hochsicherheitszone in Form eines „Fort Knox“ aufzubauen. Vielmehr geht es darum, ein professionelles Risikomanagement für den Umgang mit Informationstechnologie aufzusetzen. Dies bedeutet in erster Linie Dokumentation von Prozessen und Vorgehensweisen, sowie eine bedarfsgerechte Adressierung von identifizierten Risiken durch technische und organisatorische Maßnahmen. Hierzu gibt es unterschiedliche Methodenansätze, die von Institutionen aller Größenordnungen mit angemessenen und verhältnismäßigen Aufwänden angewandt werden können.

Darüber hinaus ist es allerdings aus Anforderungen des Datenschutzes gemäß Bundesdatenschutzgesetz (BDSG-alt, BDSG-neu) sowie der Europäischen Datenschutz-grundverordnung (EU-DSGVO) an vielen Stellen notwendig eine Folgenabschätzung vor dem Einsatz einer bestimmten Technologie vorzunehmen, um bereits im Vorfeld der Nutzung Risiken identifizieren und bewerten zu können.

Fazit

Sprichwörtlich gilt bereits, dass nur durch geeignete und regelmäßige Vorsorgeuntersuchung Krankheitssymptome erkannt werden können und die Chance für eine schnelle Gesundung besteht. Dies ist weitgehend uneingeschränkt auch auf den Einsatz von digitalen Technologien übertragbar. Und auch hier ist die frühzeitige und richtige Erkennung von Symptomen wesentlich, um Gegenmaßnahmen ergreifen zu können. Gegen eine Vielzahl von Krankheitserregern sind Impfungen eine wirkungsvolle Prävention, in Bezug auf digitale Schädlinge sind Anti-Viren-Programme aufgrund der hohen Mutationsgeschwindigkeit leider weniger effizient. Umso stärker können wir aber durch bewussten Umgang mit moderner Technologie deren Nutzpotentiale ausschöpfen, Risiken erkennen und zumeist vermeiden oder deren Eintrittswahrscheinlichkeit durch geeignete Maßnahmen verringern.