Träger I

Sicherheit kann als Treiber dienen

Jana Paul
ist Geschäftsführerin der SRH IT Solutions Heidelberg.
jana.paul@srh.de

➤ IT-Sicherheit ist in keinem Unternehmen optional, sondern stets zwingend notwendig. Für Kliniken gilt das in besonderer Weise, wie uns zunehmende Berichte von Hackerangriffen zeigen. Der Schutz vor Hackerangriffen verhindert die Unterbrechung wichtiger klinischer Prozesse und eine daraus möglicherweise resultierende Gefährdung der Patientengesundheit.

Während derzeit im Gesundheitswesen die Digitalisierung vorangetrieben wird, spielt die IT-Sicherheit eine entscheidende Rolle. Hier stehen zahlreiche Instrumente zur Verfügung, wie etwa Systeme zur Erkennung eines aktiven Angriffs und zur präventiven Verhinderung von Angriffen mit stärkeren Schutzwällen und Abwehrmechanismen. Auch Systeme zur ergonomischen und sicheren Anmeldung an IT-Systemen, etwa über Biometrie-Merkmale wie Fingerabdrücke oder Chipkarten ohne aufwendige Eingabe von Userkennung oder Passwort in Kombination mit Identitäts- und Zugriffsmanagement sind nur eine kleine Auswahl aus dem Werkzeugkasten der IT.

Die Langsamkeit der Digitalisierung ist nicht originär mangelnder IT-Sicherheit zuzuschreiben. Häufig ist es noch mehr die vollständige Umsetzung aller datenschutzrechtlichen Aspekte, die einen Geschäftsbetrieb ausbremsen kann. Tatsächlich aber steht die IT-Sicherheit nicht im Widerspruch zur Digitalisierung, sondern kann durchaus als Treiber dienen.

Das Krankenhauszukunftsgesetz schreibt einen zwingenden Anteil von 15 Prozent für förderfähige Maßnahmen für IT-Sicherheit vor. Das zeigt, wie wichtig sie als Weichensteller für die Digitalisierung ist und dass Träger sie im Gleichschritt mit der Digitalisierung ausbauen sollten. Das gelingt am besten, indem sie nur Maßnahmen in den Fördertatbeständen umsetzen können, die nachweislich technisch oder organisatorisch zu einer Erhöhung der IT-Sicherheit beitragen. Ein Beispiel wäre eine Maßnahme wie Network Access Control, bei der sich nur zugelassene Endgeräte im Netz anmelden dürfen. ▬

Träger II

Nachlässigkeit bremst aus

Stanislaw Wieser
ist Chief Information Security Officer der St. Augustinus Gruppe.
s.wieser@ak-neuss.de

➤ Eine der größten Baustellen im Gesundheitswesen ist die Digitalisierung. Das zeigt sich besonders während der Coronapandemie. Vieles läuft richtig, doch in einigen Bereichen gibt es Nachholbedarf. Besonderes Augenmerk sollte auf der IT-Sicherheit liegen. Wird sie vernachlässigt, kann das den Fortschritt verlangsamen.

Vertraulichkeit, Integrität und Verfügbarkeit aller Informationen und Systeme – dafür steht die IT-Sicherheit. Doch häufig sehen Krankenhäuser diese Bedarfe als lästige Kostenfaktoren und behandeln sie nur am Rande. Für Digitalisierungsprojekte ist das hinderlich. Nicht selten erkennen Verantwortliche zu spät ein nicht vertretbares Risiko. Das kann dazu führen, dass Projekte scheitern oder gut funktionierende Prozesse in digitale Einzelteile fragmentieren.

Im Gesundheitswesen gibt es dafür genügend Beispiele: So haben manche Kliniken bei der Aktendigitalisierung eben nicht auf gesicherte Verfügbarkeit und Vernetzung geachtet. Das führte zu digitalen Datensilos, die in weiteren Prozessen nicht mehr nutzbar sind. An eine Integration der Daten aus digitalisierten Akten ist da fast nicht mehr zu denken. Vom Papierlesen zum Bildschirmlesen, das ist wahrlich kein vorzeigbares Projekt.

Als guter Standard sollte deshalb folgender Maßstab gelten: Die technische Sicherheit muss zwingend gegen alle Formen missbräuchlichen Datenklaus und möglicher Kompromittierung geschützt sein. Das gilt für jegliche Software, Hardware und Netzwerke. Eine mangelhafte oder gar fehlende technische Sicherheit führt zu vollkommen abgeschotteten, nicht kommunikativen Systemen. Jede Form der Abschottung ist für Digitalisierungsprojekte schädlich. Eine zuverlässige IT-Sicherheit mag kostspielig sein, ist aber zwingend notwendig, um volldigital unterstützte Prozesse aufzubauen und zu beschleunigen und so deren ständige und gesicherte Verfügbarkeit zu gewährleisten. ▬

IT-Verband

Ohne Sicherheit keine Akzeptanz

Michaela Grundmeier
ist Vorstandsvorsitzende des Fachverbandes Informationstechnologie in Sozialwirtschaft und Sozialverwaltung (Finsoz).
michaela.grundmeier@finsoz.de

➤ Für uns ist IT-Sicherheit ein grundlegender Baustein der Digitalisierung. Ohne ausreichende IT-Sicherheit in der Umsetzung von Digitalisierungsvorhaben wird es im Gesundheitswesen keine Akzeptanz von digitalen Produkten und Prozessen geben. Die in jüngster Zeit bekannt gewordenen Hackerangriffe, die teils ganze Kliniken lahmlegten, legen Zeugnis dafür ab.

Es ist daher elementar, dass die Branche das Thema IT-Sicherheit professionell angeht – was nicht zwingend bedeutet, dass sich der Prozess der Digitalisierung damit verlangsamt. Im Gegenteil: Eine konzeptionell gute Vorarbeit beschleunigt die Prozess- und im Nachgang die Geschäftsergebnisse.

Es reicht nicht aus, dass IT-Sicherheit von IT-Mitarbeitenden oder IT-Leitungen in den Einrichtungen und Trägerorganisationen einfach nur mitgemacht wird. IT-Sicherheit muss von Grund auf konzipiert werden. Der Aufbau eines IT-Sicherheitsmanagements sollte die Basis des Konzeptes bilden. Wichtig sind auch Kenntnisse über mögliche IT-Angriffsszenarien. Unternehmen müssen Wissen und Know-how kurzfristig aufbauen und langfristig finanzieren. Auch der Weg in die Cloud nimmt den Unternehmen nicht die Verantwortung ab, sich mit IT-Sicherheit zu beschäftigen. Denn Cloud-Anbieter sind nicht für die Sicherheit der Daten verantwortlich. Das ist und bleibt Aufgabe des Unternehmens.

Eine mangelnde IT-Sicherheit wird aus meiner Sicht die Digitalisierung nicht verlangsamen, sondern sie im Gegenteil stark gefährden. Die Fachgruppe IT-Compliance des Digitalverbandes Finsoz beschäftigt sich daher aktuell mit dem Thema. Denn Organisationen benötigen Unterstützung dabei zu verstehen, wie IT-Sicherheitsmanagement funktioniert. ▬

Politik

Absoluter Schutz ist nicht möglich

Prof. Dr. Jörg Debatin
ist Leiter des Health Innovation Hub des Bundesgesundheitsministeriums.
info@hih-2025.de

➤ Ja, es ist die Stunde der digitalen Medizin. Die Coronapandemie wirkt als Booster dieser Entwicklung. Neu ist, dass der Nutzen digitaler Anwendungen für alle erstmals erlebbar ist. Das wiederum rief naturgemäß diejenigen auf den Plan, für die Datenschutz das Allheilmittel gegen jegliche Veränderungen ist. Videosprechstunden seien beispielsweise aus Sicht des Datenschutzes ein Einfallstor in die Privatsphäre. Allein der Beweis wurde nicht angetreten.

Der Schutz persönlicher Daten ist wichtig. An unseren Grundwerten einer freiwilligen Teilnahme an der Datensammlung dürfen wir nicht rütteln, auch nicht in einer Krise. In Deutschland haben wir ein strenges Verständnis im Umgang mit Daten. Auch deshalb haben wir mit der Telematik-Infrastruktur als weltweit einziges Land eine eigene Datenautobahn für Gesundheitsdaten geschaffen. Und dennoch muss vollkommen klar sein: Es gibt keine absolute Sicherheit im Umgang mit Daten, übrigens genauso wenig wie im Umgang mit Papier.

Wir brauchen ein angemessenes Verhältnis zwischen Datenschutz und Datensicherheit auf der einen sowie Gesundheitsschutz auf der anderen Seite. Dabei sollten wir nicht vergessen, dass die Verfügbarkeit von Daten Grundlage einer guten Gesundheitsversorgung ist. Ohne Datenverfügbarkeit nehmen Patientinnen und Patienten Schaden. Die Entstehung der Corona-Warn-App hat eindrücklich gezeigt, dass die beiden Ziele Virenschutz und Datenschutz gemeinsam realisiert werden können.

Meine Empfehlung ist, dass wir digitale Wege öffnen sollten, ohne dabei unsere Grundwerte zu opfern. Wenn die Menschen erleben, dass die Digitalisierung in der Medizin praktisch und effizient ist, Zeit spart und dabei hilft, schneller gesund zu werden oder die Gesundheit besser zu erhalten, dann gehört die Digitalisierung für mich als integraler Bestandteil der medizinischen Versorgung in Deutschland dazu. ▬