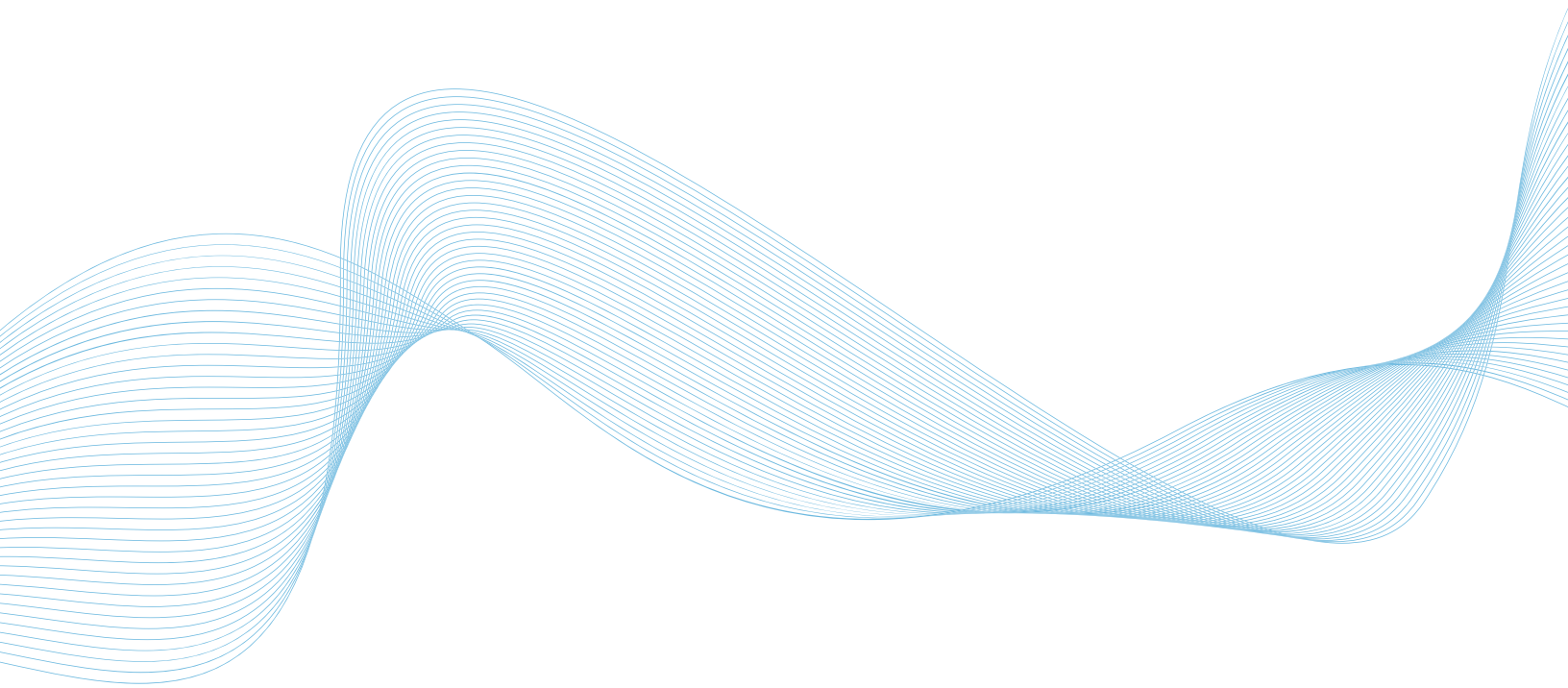
netwrix

Frank Stratmann und Jeff Melnick

Das Krankenhaus und Gesundheitsdaten

Herausforderungen im Umgang mit Daten in Gesundheitsbeziehungen an der Schnittstelle Patient und klinischer Einrichtung



Frank Stratmann

Mitglied des Vorstands und Pressesprecher, Bundesverband Internet-medizin e.V., Mentor & Personal Digital Officer, Xing Ambassador für Gesundheit

Jeff Melnick

IT-Sicherheitsexperte, Netwrix

Aktion

Netwrix im Gesundheitswesen

Effektive Datensicherheit und Nachweis der Compliance kostenlos für 3 Monate

für alle Organisationen im Gesundheitswesen

Jetzt anmelden

Inhaltsverzeichnis

Teil 1

Das Krankenhaus und Gesundheitsdaten

Teil 2

Datensicherheit für elektronische Patientenakten

Teil 1

Das Krankenhaus und Gesundheitsdaten

Zusammenfassung

Der Umgang mit Gesundheitsdaten jeglicher Art stellt Krankenhäuser vor besondere Herausforderungen. IT-Abteilungen in Krankenhäusern stehen vor Veränderungen, die mit dem Wandel einer sich ändernden Gesundheitskultur begründet werden können.

Es wird zu klären sein, was Gesundheitsdaten sind, warum ein Krankenhaus eingestellt sein muss auf den Umgang mit Daten von außerhalb der eigenen Einrichtung und welche Auswirkungen das auf das Geschäftsmodell Krankenhaus mit sich bringt.

Dieses Whitepaper bietet IT-Verantwortlichen eine Begründungshilfe, um im Unternehmen Unterstützer zu finden, mittelfristig die richtigen Entscheidungen vorzubereiten und zu treffen. Es erklärt auch in einer kulturellen Dimension, warum die Bedeutung von Gesundheitsdaten im Krankenhaus zunimmt.

I. Medizin und Daten

Medizin war nicht immer wissenschaftlich, aber stets eine Disziplin, die ohne Daten nicht auskam. Viele Jahrtausende lag das Wissen im Kopf der an der Heilung von Kranken beteiligten Experten. Wissen wurde überliefert und später aufgeschrieben. Am Ende der Gutenberg Galaxis verfügen wir über immer mehr Daten, die elektronisch oder digital gespeichert werden und damit einen neuen Anreiz ihrer Verfügbarkeit und Nutzung versprechen.

Die Digitalisierung verändert, wie Gesundheit gelingt.

Beim elektronischen Speichern darf auf Papier verzichtet werden. Das birgt Herausforderungen bei der Langzeitarchivierung, fördert jedoch die Distribution von Daten, die heutzutage an vielen Orten gleichzeitig benötigt werden oder nach Ihrer Erhebung und Nutzung einem anderen Zweck zugeführt werden. Das Verschränken von Daten in der Medizin zu Big Data verspricht neue Evolutionssprünge für den Fortschritt der Medizin. Künftig wird Technologie dabei helfen Krankheiten besser zu verstehen. Dabei gewinnen vor allem Daten von außerhalb des Krankenhauses an Bedeutung.

Wer in der Geschichte der Medizin weit genug in die Vergangenheit forscht, ist wenig überrascht, dass der Ursprung der heutigen wissenschaftlichen Medizin auf Hippokrates zurückgeht[1]. Die Vorgehensweise aus Anamnese, Diagnose, Therapie und Prognose hat sich in den zurückliegenden Jahrhunderten gewandelt. Doch die Lernkurve der medizinischen Entwicklung springt mit dem methodischen Einzug der Wissenschaft spätestens seit der Industrialisierung nicht mehr launisch hin und her. Mit dem Einzug an modernen Verfahren und Methoden schwingen sich Forschung und Entwicklung in der Medizin auf eine stetige Entwicklung ein. Die gerade exponentiell wachsende Datenverarbeitungsgeschwindigkeit verleiht dieser Entwicklung einen weiteren Innovationsschub.

Daten als Attraktion

Die Anforderungen an die Datenqualität und die Herausforderungen an die Datensicherheit und den Datenschutz erlauben seit jeher keine falschen Kompromisse. Daten sind essentiell für ein modernes Unternehmen. Entstanden elektronische Daten früher durch die Bewältigung von Medienbrüchen zwecks Archivierung, werden sie heute als Ressource und Kapital ausschlaggebend für den wirtschaftlichen Erfolg. Die Entstehung des Fachs Medizin-Controlling steht dafür. Daten versprechen einen Wettbewerbsvorteil. Aber nur für den, der es versteht, Daten im Innen- und Außenverhältnis zu nutzen.

Jeder durch Datenerhebung erschlossene Wettbewerbsvorteil würde kompensiert, wenn der korrekte Umgang mit Daten fehlt. Im Krankenhaus finden sich Daten derzeit in unterschiedlichen Systemen. Daraus lässt sich ein passiver Schutzstatus ableiten. Verstreute, nicht gebündelte Daten sind weniger attraktiv. Das schützt vor Diebstahl und Missbrauch. Sobald allerdings Daten aggregiert werden - und davon ist in Zukunft

auszugehen - steigt die Attraktivität. Der Aufwand um die Sicherstellung der jüngst eingeführten DS-GVO hat gezeigt, wie komplex das Thema bleibt.

Vor allem wenn Fallakten mehr sein werden als abrechnungssensitive Dokumentationen. Hier müssen Sicherheitsstandards geschaffen werden, um einen mutwilligen oder fahrlässigen Abfluss von Gesundheitsdaten über ungesicherte Schnittstellen zu vermeiden. Sobald Daten an einem zentralen Ort strukturiert gesammelt werden, steigt die Gefahr Zielscheibe für Angriffe zu werden.

Hinzu kommt die Nutzung des technologischen Fortschritts, der auch die medizinische Leistungserbringung erreichen wird. Daten auf die nicht zugegriffen werden kann, weil sie nicht zur Verfügung stehen, schaden der Zukunftsfähigkeit des Unternehmens Krankenhaus.

Die Digitalisierung passiert. Daten sind dabei nicht nur Outcome, sondern drehen sich quasi um sich selbst. Vergleiche mit dem Rohöl der gerade ausklingenden Epoche sind geduldig und viele sind nicht ohne Grund von diesem Bonmot genervt. Doch die Bedeutung von Daten ist unumstritten. Daten fördern neue Geschäftsmodelle oder schaffen positive Anreize, das eigene Geschäftsmodell weiterzuentwickeln.

Jedes Krankenhaus - egal wie es heißt - trägt seine soziale Verantwortung im Namen.

Daten sind Teil des Krankenhauses der Zukunft. Das finden manche nur schwer attraktiv, weil der Einfluss von außen zunimmt und Daten durch ihr flüchtiges Wesen die Vorstellung zerstören, alles bliebe - wie immer - an seinem gewohnten Platz. Veräußerte Daten lassen sich nicht wie ein Stück Papier zurückholen. Die Dezentralisierung der gesundheitsbezogenen Daten gewinnt an Fahrt. Die Deutungshoheit von Daten obliegt nicht mehr allein dem Arzt. Sogar dann nicht, wenn es um die Qualität einer medizinischen Leistung des eigenen Krankenhauses geht. Das verändert Krankenhäuser ohne sie von der Pflicht zu entbinden, eine qualitative Versorgung sicherzustellen. Und dazu werden in Zukunft Daten berücksichtigt, die nicht nur im eigenen Krankenhaus erhoben wurden.

Ein weiterer Aspekt und auf den legt dieses Whitepaper ein besonderes Augenmerk: Daten müssen eine neue Wertschöpfung erfahren. Medizin ist datengetriebener denn je. Und Daten sind heute digital. Die Digitale Medizin sucht ihren Platz in der Wertschöpfungskette auch in Krankenhäusern.

Anmerkungen

Fn. 1 | Vgl. Pohlenz, M. (1938) Hippokrates und die Begründung der wissenschaftlichen Medizin. De Gruyter.

II. Definition und Unterscheidung von Gesundheitsdaten

Gesundheitsdaten als Wort ist heute noch ein schwammiger Begriff über dessen Bedeutung wir erst in einigen Jahren mehr erfahren. Nämlich dann, wenn wir erkennen, was die Tech-Unternehmen wirklich tun, wenn sie uns Armbänder, smarte Uhren oder andere Sensorik in Gadgets verstecken mit denen wir uns selbst vermessen. Sie sind die waren Vermesser von Gesundheit.

Personenbezogene Daten

Laut DS-GVO gehören Gesundheitsdaten zur Kategorie der besonders schützenswerten personenbezogener Daten. Im Prinzip wird die Verarbeitung sogar untersagt, es sei denn der Patient stimmt der Verarbeitung ausdrücklich zu. Krankenhäuser haben sich damit im Zuge der Umsetzung der Bestimmungen zur DS-GVO intensiv auseinandersetzt.

Dabei fällt dem Krankenhaus per Gesetz eine besondere Rolle zu. Denn Sie sammeln pro Jahr über 19 Millionen Deutschland vollstationäre Daten nach DS-GVO § 9 Absatz 2 h. Hinzu kommt die Zahl der ambulanten Fälle. Interessant in diesem Zusammenhang sind die Ergebnisse des ePatient Survey 2018, die wir im Kapitel zu den Patientenakten näher beleuchten. Was oft missverstanden wird. Ein erweiterter Datenschutz personenbezogener Daten zu Gesundheitsfragen verbietet nicht per se das Sammeln. Sie genießen nur einen besonderen Schutz, der auch dann sichergestellt sein muss, wenn eine vielfältige Nutzung der Daten in unterschiedlichen Kontexten gewünscht ist. Wenn dieses Whitepaper die These aufstellt, dass Gesundheitsdaten eine größere Rolle spielen werden, muss diese Tatsache stets berücksichtigt werden.

Zu den personenbezogenen Daten gehören auch all jene Daten, die einen Rückschluss auf eine bestimmte Person zulassen.

Gesundheitsdaten

Der Begriff Gesundheitsdaten suggeriert schon, dass die Daten nicht zwingend etwas mit Krankheit zu tun haben müssen. Ein Blick in die Szene der Selbstvermesser macht das sichtbar. Anhänger der Quantified Self Bewegung sammeln nicht nur Gesundheitsdaten, aber vor allem und gern diese Art der personenbezogenen Daten.

Als Gesundheitsdaten werden heute alle Daten bezeichnet, die im Zusammenhang mit dem gesundheitlichen Zustand einer Person erhoben und verarbeitet werden.

Personenbezogene Daten

Vitaldaten sind Messergebnisse, die mithilfe von Medizintechnik erhoben werden und die Grundfunktionen des menschlichen Körpers widerspiegeln. Erst mithilfe eines geeigneten Referenzwertes können sie eingeordnet werden. Je nach Korrelation mit anderen Vitalwerten kann dann ein Bezug zu einem Gesundheitszustand hergestellt werden.

Körperbezogene Maßzahlen

Werte wie der BMI zählen wir zu den körperbezogenen Maßzahlen. Sie ergeben sich aus der Berechnung gemessener Vitalparameter und geben in Verbindung mit Referenzwerten ebenso Auskunft über den Gesundheitszustand einer Person.

Krankheitsbezogene Daten

Zu den Krankheitsdaten gehören alle Daten, die im Rahmen einer ambulanten oder klinischen Anamnese, Diagnose und Therapie im Kontext einer Indikation erhoben und verarbeitet werden.

Im Krankenhaus fallen im Normalfall alle oben beschrieben Datenarten an. Wir beschränken uns in diesem Whitepaper daher auf die Benennung von Gesundheitsdaten.

III. Gesundheitsdaten sind nicht gleich Daten

Im wesentlichen unterscheiden wir für Gesundheitsdaten holzschnittartig zwischen strukturierten Daten und anderen Daten. Strukturierte Daten sind dabei in der Regel Datensätze, die ein bestimmtes Format einhalten, um gemeinsam mit weiteren Daten verarbeitet werden zu können.

Andere Daten sind z.B. aus einem Medienbruch stammende Daten. Die digitale Abbildung, das Röntgenbild oder ein digitaler Arztbrief können zu dieser Datenart gezählt werden.

Anonymisierung & Pseudonymisierung

Unter Anonymisierung versteht man das Verändern personenbezogener Daten dergestalt, dass diese Daten nicht mehr einer Person zugeordnet werden können. Der Personenbezug wird also aufgehoben.

Bei der Pseudonymisierung werden Name und/oder andere Identifikationsmerkmale durch ein Pseudonym ersetzt. Dadurch wird ein Rückschluss auf eine bestimmte Person weitestgehend ausgeschlossen oder zumindest erschwert.

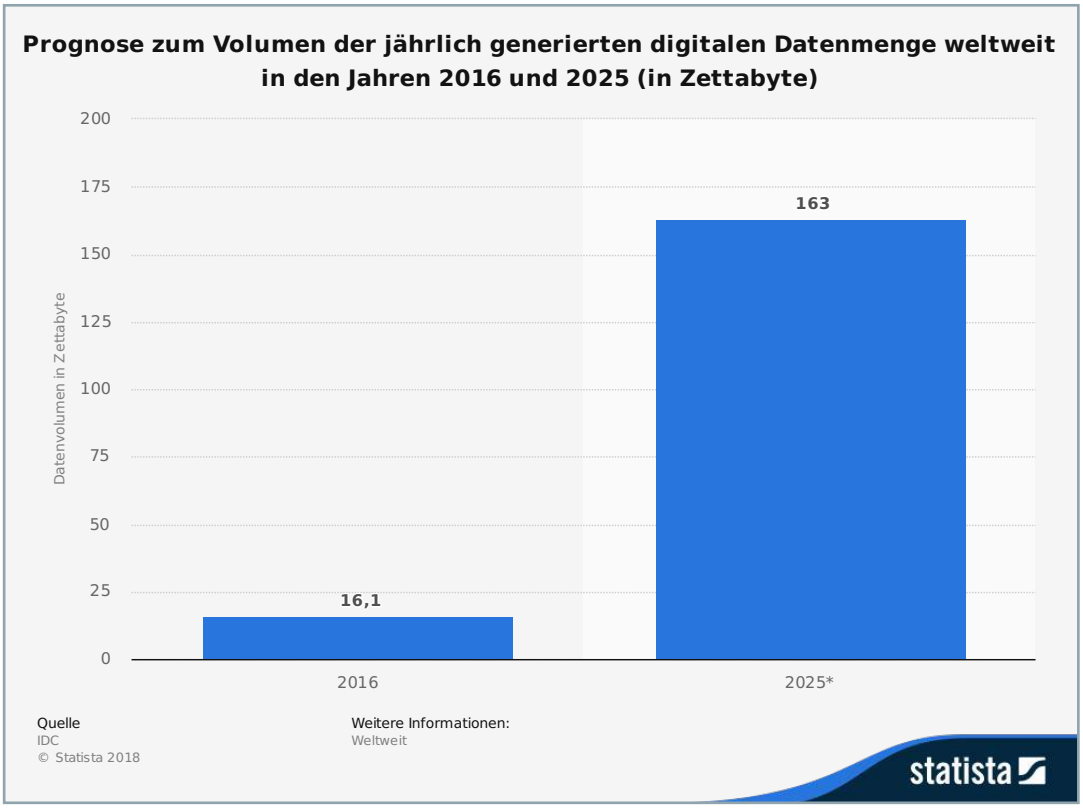
Datenvolumen

Mit welcher Größenordnung an Datenvolumina die heutige Medizin umzugehen hat, hätten sich die Heilkundigen der Antike sicher nicht vorstellen können. Bei einem Krankenhausaufenthalt entsteht heute eine Datenmenge, die mehr als 12 Millionen Romanen entspricht. Dies sind Dimensionen, die ohne IT-Technologie gar nicht mehr bewältigt werden könnten[2]. Hinzu kommen künftig Daten aus einem Krankheitsverlauf der pre- und zurückliegenden poststationären Aufenthalten. Laut ePatient Survey 2018 wünscht sich der Patient eine verständliche und relevante digitale Orientierung von seinen Behandlern während und nach seiner Therapie. Dabei steigt die Relevanz externer Daten stetig.

Wenn wir in einigen Jahren auf das sich heute abzeichnende exponierte Wachstum der Datenmengen und ihrer verschränkten Verwendung zurückblicken werden, wird sich auch die Welt der Health-IT verändert haben. Mit dieser Überlegung darf angenommen werden, dass der Health-IT künftig eine besondere Rolle zufällt. Eine agile und zielführende Nutzung von Daten durch medizinische Experten ist nur möglich, wenn der Medizin eine zeitgemäße Health-IT zur Verfügung steht.

Abb. 1 Prognose zum Volumen der jährlich generierten digitalen Datenmenge weltweit in den Jahren 2016 und 2025 (in Zettabyte)

Die Statistik befasst sich mit dem jährlichen digitalen Datenaufkommen bis 2025. Laut Quelle soll sich das Datenaufkommen im Jahr 2025 auf 163 Zettabyte belaufen.



Health IT

Informatik und Medizin gehen erst seit den 1970er Jahren Hand in Hand. Der erste Studiengang in medizinischer Informatik wurde von 22 Studierenden im Wintersemester an der Hochschule Heilbronn 1972/1973 besucht. Beworben hatten sich immerhin 45 Bewerber. Insgesamt war der Kooperationsstudiengang der damals erste grundständige Studiengang im Bereich der Medizinischen Informatik weltweit[3]. Ergänzend zu den etablierten Disziplinen heißen die Disziplinen heute Machine- und Deep-Learning und sie ermöglichen immer häufiger Anwendungsszenarien für eine Medizin, die vor der Herausforderung steht, den eigenen Fortschritt zu sichern und dabei weniger administrative Kosten zu erzeugen.

Anmerkungen

Fn. 2 | Vgl. Langkafel, P. (Hrsg. (2014) Big Data in Medizin und Gesundheitswirtschaft. medhochzwei Verlag.

Fn. 3 | Vgl. 40 Jahre Medizinische Informatik (2013).
Available at: https://40jahre.mi.hs-heilbronn.de/index.php/40jahremi-hintergrund (Accessed: 4 September 2018).

Abb. 1 | Vgl. https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/

IV. Unterschiedliche Perspektiven auf Gesundheitsdaten

Wie eingangs erwähnt, kommt Medizin nicht ohne Daten aus. Für Ärzte ist das nichts Neues. Auch Patienten interessieren sich neuerdings für die Daten rund um Ihre Gesundheit und Krankheit. Warum aber haben große Tech-Unternehmen plötzlich auch ein Interesse an den Daten rund um unseren physische Zustand? Wirklich nur um uns kontextsensitive Werbung anzuzeigen oder Ärzten und Krankenhäusern in Deutschland das Leben schwer zu machen?

Das Auftauchen der neuen Player im Gesundheitsmarkt wird regelmäßig falsch eingeschätzt. Der Arzt denkt, Dr. Google mache ihm Konkurrenz in seiner Rolle als Aufklärer. Der Patient will nicht mehr auf den Konsum von Informationen rund um sein Leiden verzichten. Manche gesunde Menschen steigern sich in hypochondrischen Exzessen in Krankheiten hinein. Die Technologieriesen allerdings haben tatsächlich keine Ahnung von medizinischer Leistungserbringung. Sie denken vollständig anders, was ihnen erlaubt, sich der Grundthematik einer gelingenden Gesundheit auf ihre Weise zu nähern.

Das alles hat mit der Mathematisierung unserer Welt zu tun. Was wir erklären wollen, versuchen wir mit Zahlen darzustellen, weil wir glauben, es würde dadurch vorstellbarer. Martin Heidegger sagte einst »Die Wissenschaft denkt nicht«. Er meinte das nicht als Vorwurf. Der Satz diente ihm zur Feststellung der inneren Struktur der Wissenschaft. Wer forscht, denkt vielleicht nicht an die Technik, die mit dem geschaffenen Wissen so etwas hervorbringt wie die Atombombe. Die Weltgeschichte kennt viele Beispiele wo mit Wissen eine Technik erschaffen wurde, die das eine Mal extrem hilfreich sein kann und ein anderes Mal sein zerstörerisches Potenzial entfaltet.

Längst hat sich das Wesen der Wissenschaft auf unsere Alltag übertragen. Auch in Gesundheitsfragen. Natürlich gibt es auch Menschen, die sich von der wissenschaftlichen Erkenntnis nur überzeugen lassen, wenn sie evident ist. So erklären sich die Grabenkämpfe zwischen Homöopathianhängern und den Globulisierungsgegnern. Darunter naturgemäß viele Ärzte. Wissenschaft verändert den Wahrheitsgehalt. Je nach dem mit welcher Perspektive ich mir meine Welt konstruiere.

Die wissenschaftliche Ausbildung des Arztes, der später unmittelbar am Patienten wirkt, also buchstäblich operativ tätig wird, findet nur sehr selten den Weg über die Technik ins Krankenhaus oder die Praxis. Die Medizintechnik hat sich im letzten Jahrhundert enorm entwickelt, hat sich dabei aber vor allem auf Ausrüstung für medizinische Experten konzentriert. Selbstverständlich richtet die Medizintechnik Ihre Angebote auch an Konsumenten als Nutzer. Denken wir an das Fieberthermometer, das heute in jeder Hausapotheke liegt. Oder an Messgeräte für Blutzucker und Blutdruck. Diese genannten Beispiele für einfach handhabbare Medizintechnik dienen uns, das oben Gesagte besser zu verstehen. Wir lesen den Wert ab und haben Fieber, Bluthochdruck oder Diabetes. Wir erzeugen einen Wert für das, was in der Lesart

der Mathematik nicht vom Körper angezeigt wird. Ein Unwohlsein lässt sich aus dem Körper heraus beschreiben, aber es braucht Hilfsmittel, um diese sinnliche Lesart in rationale Zahlen zu verwandeln.

Konsequenterweise müssen wir bei Messergebnissen der Medizintechnik von Krankheitsdaten (s.o.) sprechen, wenn sich aus den Werten eine Indikation ableiten lässt. Sollte - trotz Messung - keine Krankheit vorliegen, würde wir von Vitaldaten sprechen, die keinen Anlass bieten, nervös zu werden.

Vermesser wird also nicht eine Krankheit, sondern Gesundheit.

Am Beispiel der Apple-Watch lässt sich das gut erklären. Die Apple Watch ist eines der ersten Geräte, das sich nicht nur als Lifestyle sondern auch als Healthstyle[4] Produkt kategorisieren lässt. Durch die Integration sogenannter Quantified-Self-Technologien gibt die Apple Watch engmaschig Auskunft über die Vitaldaten seines Trägers. Erlaubt der Träger dieser Uhr die Übermittlung dieser Daten an Apple wird daraus eine wissenschaftliches Projekt aus dem später Gesundheitsservices für den Nutzer abgeleitet werden können. In einem ersten Schritt ist das z.B. die Teilnahme an einer Studie. Diese wurde bereits mit der Einführung der Apple Watch Series 3 gemeinsam mit Stanford Medicine zur Erkennung von Herzinsuffizienz angeboten. Eine simple Meldung auf dem Display der Uhr, der Patient leide möglicherweise an Herzinsuffizienz, wirft den Menschen anders als früher in eine Krankheit.

Nehmen wir die Perspektive der Tech-Unternehmen ein, wird klar, dass sie kein Interesse haben, Daten zu erheben, die auf einen Krankheitszustand hindeuten. Die Apple Watch misst, ob sein Träger gesund ist. Erst mit wissenschaftlichen Erkenntnissen, die weiterhin aus der medizinischen Forschung kommen werden, gelingt das, was die Medizin allein nicht kann. Die engmaschige Vermessung des Menschen erlaubt es, einen Musterwechsel durch Abweichung zu erkennen. Vorhofflimmern oder Diabetes werden dann einfach berechnet. Spätestens dann ist der Weg nicht mehr weit, neue Heilungsoptionen zu designen oder der Medizin einzuflüstern, wie es besser gelingt, eine Krankheit zu handhaben.

Die Nutzerzahlen sind heute schon der Anzahl der Studienteilnehmer tradierter, wissenschaftlicher Methodik überlegen.

Anmerkungen

Fn. 4 | Vgl. 1999 erstmalige Erwähnung des Begriffs Healthstyle im wissenschaftlichen Kontext durch Porter Novelli Healthstyles Survey | Gateway to Health Communication | CDC (1999). Available at: https://www.cdc.gov/healthcommunication/toolstemplates/entertainmented/1999Survey.html (Accessed: 6 September 2018).

V. Das Krankenhaus als datengetriebenes Unternehmen

Die Neubewertung von Daten für den klinischen Betrieb lässt sich für das Krankenhaus als datengetriebenes Unternehmen besser verstehen, wenn man sich anschaut, wie die Geburt der modernen Klinik eingeläutet wurde. Um 1867 erhielt das bereits erwähnte Fieberthermometer seine Bedeutung zur Objektivierung der Körpertemperatur. Vor über 150 Jahren wird es buchstäblich zwischen den Patienten und den Arzt geschoben, wenn es auch unmittelbar am Patienten Anwendung fand. Doch seine Bedeutung ist nicht geringer einzustufen als die heutigen, medizintechnischen und smarten und immer öfter sensorischen Möglichkeiten zwischen selbigen am Gesundheitsgeschehen beteiligten Akteuren. Immer schon wurden Daten erhoben und Daten wurden interpretiert, um auf ihrer Basis Diagnose, Therapie und Prognose zu formulieren. Die heutigen Möglichkeiten rangieren zwischen einfachster Sensorik und millionenschwerer Medizintechnik, z.B. bei bildgebender Diagnostik oder dem Da-Vinci-Operationssystem. Dabei wird immer unklarer, wer das Instrument in der Hand hält. Der Computer-Topograph (CT) wird wohl noch lange von ausgebildetem Fachpersonal bedient. Doch wie steht es mit der Vorhersage der Indikation Vorhofflimmern durch die Apple Watch[5]?

Die Einführung des Fieberthermometers

Das Fieberthermometer wurde in seiner Bedeutung genau so unterschätzt wie heutige, teils einfachste Apparaturen, die von Patienten - ähnlich wie das Fieberthermometer - selbst bedient werden können. Im Falle des Fieberthermometers trug sich das wie folgt zu:

Man deutete auf die Anzeige und las die Wahrheit ab. So schien es jedenfalls.

Solange der Arzt den Körper eines Erkrankten mit den eigenen Sinnen erforschen musste, beispielsweise durch Handauflegen im Bereich der Stirn, reduzierte sich seine Kunst auf das rein subjektive Vermögen, Fieber korrekt zu diagnostizieren. Während der erste Arzt ein *feuriges Fieber* attestierte, kam ein zweiter Kollege vielleicht zu dem Schluss, es läge *nur eine erhöhte Temperatur* vor. Als nun das Fieberthermometer als Instrument im Raum zwischen Patient und ärztlicher Kunst auftauchte, las man ab, ob der Patient an Fieber leidet oder eben nicht.

Die gesicherte Erkenntnis, dass ein Patient im Ergebnis eine Körpertemperatur von 39,8 Grad vorzuweisen hatte, veränderte den Charakter, wie Diagnosen und in der Folge Therapien und Prognosen auszufallen hatten. Das Fieberthermometer war also so etwas wie ein neues Medium, was zu einer völligen Neubewertung führte. Die Geburtsstunde der modernen Klinik. Statt langer Überredungsversuche, Erklärungen und Debatten zeigte man einfach auf den (An)Zeiger. »Konsens per Fingerzeig« sozusagen. Die neue Form der Demonstratio. Das machte das Fieberthermometer (und in seiner

Folge andere Instrumente) zu gerade unerhört effizienten und darum begehrten Medien wissenschaftlicher wie technischer Kommunikation[6].

Digitalisierung und Medialisierung

Aus diesem Grund darf im Zuge der Digitalisierung die fortschreitende Medialisierung nicht übersehen werden. In einem Krankenhaus fällt der Digitalisierung ein strategisches und taktisches Kalkül zu. Vergessen werden darf nicht, dass sich mit der Einführung von Instrumenten der Digitalisierung, die nicht mehr nur durch den Arzt bedient werden, der Rhythmus im Verhältnis zwischen Arzt und Patient verändert. Auch im stationären Alltag gehören von Patienten eingebrachte Gadgets, die Gesundheitsdaten erzeugen zur Üblichkeit.

Daten werden nicht mehr isoliert hoheitlich erhoben, sondern wollen zwischen Arzt und Patient geteilt werden. Damit ergeben sich neue Aufgabenstellungen, auf die wir noch eingehen werden.

Wer von der Digitalisierung spricht, sollte im Krankenhaus nicht nur an die Prozesswelt denken. Auch wenn ein Krankenhaus heute bereits mit sehr vielen Daten arbeitet. Die Integration von Daten im äußeren und internen Weltverständnis eines Krankenhauses macht ein Krankenhaus mittelfristig zu einem datengetriebenen Unternehmen. Daten aus unterschiedlichen Systemen und Komponenten fließen derzeit nur soweit ins Krankenhausinformationssystem (KIS) wie sie für die Abrechnung und Dokumentation gebraucht werden.

Wie oben bereits erwähnt, fehlt es am Vermögen, die Daten aus unterschiedlichen im Krankenhaus verfügbaren Systemen zu bündeln. Zentraler Baustein bleiben vor allem Gesundheitsdaten, die sich um den einzelnen Fall drehen und zur Kompensation von Krankheiten aggregiert und integriert werden müssen. Dabei stammen die Daten nicht immer aus dem eigenen Haus.

Medialisierung

Die Medialisierung ist unumkehrbar und demokratisiert die Informationslandschaft für Gesundheit weiter. Die Hoheitsgebiete für Gesundheitskompetenz liegen schon länger nicht mehr im Krankenhaus oder in der Arztpraxis. Informationen werden stetig dezentralisiert und müssen jetzt strukturiert nutzbar für alle am Gesundheitsgeschehen Beteiligten gemacht werden.

Dezentralisierung

Mit den Dezentralisierungsbemühungen im Gesundheitsgeschehen und der medialen Vielfalt, steht das Gesundheitssystem vor fundamentalen Umbrüchen. Sie zeigen sich nicht als Tsunami oder Erdbeben. Es gleicht eher dem Wesen einer schleichenden Erosion.

In der Dezentralisierung liegt der Schlüssel zur Rettung unserer Versorgungsqualität. Die Kosten für eine zentralisierte Verwaltung des Gesundheitsgeschehens durch das System werden sich absehbar potenzieren, was die Dezentralisierung sinnvoll erscheinen lässt und die Bemühungen anheizen wird. Knotenpunkte für Vertrauen lösen sich auf, weil Vertrauen sich im Wert verändern wird.

Wirtschaftliche Bedeutung von Gesundheitsdaten

Gesundheitsdaten erhalten neuerdings eine Bedeutung zur taktischen Ausrichtung eines Krankenhauses in wirtschaftlicher Hinsicht. Das umfasst immer auch eine medizin-strategische Überlegung. Vor allem dann, wenn nicht mehr nur die lukrative Güte von Leistungen, die auf das Wertangebot im eigenen Haus einzahlen, berücksichtigt werden können. Seitens des Gesetzgebung erwarten wir künftig Initiativen zur Versorgungsqualität, die auch externe Gesundheitsdaten berücksichtigen könnten.

Schon heute werden Medizin-Strategien im Abgleich mit Leistungsdaten und Erwartungswerten der statistischen Landes- und Bundesämter formuliert. Die wachsende Vielfalt der Daten sorgt sicher dafür, dass man immer noch weitere Parameter berücksichtigen will. Wenn die Märkte enger sind, sucht man in den Nischen nach Daten, die den Unterschied in der Wirtschaftlichkeit bringen, wenn mithilfe schlüssiger Daten die richtigen Maßnahmen formuliert werden.

Agile Nutzung relevanter Daten

Daten sollten in einem Krankenhaus als Service zur Verfügung stehen, um beste Entscheidungen treffen zu können.

In einem datengetriebenen Krankenhaus werden Daten aus unterschiedlichen Quellen weniger exklusiv verwaltet als heute, sondern eher vielfältig zuständigen Rollen für die eigene Arbeit zur Verfügung gestellt. Es ist davon auszugehen, dass sich mit der Informationsarchitektur auch die Informationskultur in Krankenhäusern stark verändern wird. Daten werden nicht mehr vom Vorgesetzten präsentiert oder von einem kleineren Kreis genutzt, um sie ständig per E-Mail hin- und herzuschicken. In unterschiedlicher Form, profitieren mehrere medizinische, pflegerische und administrative Abteilungen von einer intelligenten Unterstützung in der Nutzung relevanter Daten.

Dabei ist - ähnlich wie heute - auf die Berechtigung des Rolleninhaber für den Zugriff zu achten. Diese Berechtigung leitet sich aus der Regel ab, ob Daten sinnvoll auch für unternehmerische Entscheidungen genutzt werden können. Doch auch hier braucht es ein Umdenken. Traditionelle Bewertungsmaßstäbe verlieren zunehmend ihre Gültigkeit. Vollständigere Marktbeobachtungen beispielsweise ergeben sich aus Daten der eigenen Leistungserbringung, die in einer Verhältnis zum restlichen Marktgeschehen gesetzt werden. Wenn auch nicht jedes Detail einer Krankengeschichte für die Auseinandersetzung mit dem Markt gebraucht wird, werden Daten des stationären Geschehens doch in administrativen Bereichen benötigt, um strategische Entscheidungen zu begründen. Auch paramedizinische Bereiche profitieren von der Zugänglichkeit.

Übersetzungsleistung von Gesundheitsdaten

Zur Aufbereitung von Rohdaten, zwecks Visualisierung oder Storytelling braucht es bestimmte Kompetenzen, die in Supportabteilungen von Krankenhäusern heute nur vereinzelt zu finden sind. Ferner fehlen ähnliche Kompetenzen in Entscheider-Gremien. Allein das Medizin-Controlling hat hier in den letzten Jahren aufgeholt, bleibt aber abhängig vom Bewusstsein des IT-Managements hinsichtlich der Bedeutung von Daten. Fehlt dieses Bewusstsein, wird es schwer, Abteilungen, die z.B. nicht unmittelbar am medizinischen Geschehen beteiligt sind, sondern das Wertangebot eines Krankenhauses allgemein verantworten, intelligent mit Daten zu versorgen.

Fehlt den Daten die Übersetzungsleistungen entstehen keine Maßnahmen.

Anmerkungen

Fn. 5 | Vgl. Stratmann, F. (2017) Herzensangelegenheit in Apple Keynote war nicht das neu vorgestellte iPhone, XING News.
Available at: https://www.xing.com/news/insiders/articles/herzensangelegenheit-in-apple-keynote-war-nicht-das-neu-vorgestellte-iphone-924920 (Accessed: 4 September 2018).

Fn. 6 | Vgl. Wasser, H. (2012) 'Die Geburt der Klinik und das Labor', in Vom Weltbild der Rhetorik, vom Buchdruck und von der Erfindung des Subjekts. Velbrück Wissenschaft, pp. 234–239.

VI. Bedeutung von Daten für das Krankenhaus der Zukunft

Derzeit unterschätzen Krankenhäuser ihre Rolle als datengetriebenes Unternehmen. Neben dem operativen Betrieb der einst als elektronischen Datenverarbeitung bezeichneten Administration eines Krankenhauses fehlt in vielen stationären Einrichtungen bis heute das Gespür, welche Bedeutung Krankenhäusern in Zukunft zufallen könnte, wenn es darum geht, als Knotenpunkt für eine datengetriebene Medizin neben der individuellen Bewältigung von Krankheit auch dem öffentlichen Anspruch in einem umfassenderen Sinne (z.B. Public Health) zu dienen. In Anbetracht der fortschreitenden Konsolidierung des Gesundheitsmaktes, Schwierigkeiten bei der Refinanzierung der Investitionen im Sinne des medizinischen Fortschritts und reformbedürftiger Finanzierung allgemein, scheinen die Digitalisierungsbemühungen wie ein weiteres Übel für alle Gesundheitsakteure. Besonders betroffen sind die Krankenhausbetreiber. Sie stehen im Vergleich zu vielen absatzorientierten Unternehmen doppelt in der Verantwortung. Ein Gelingen von Gesundheit ist immer ein Prozess zwischen Medizin und Mensch. Zwischen Arzt und Patient. Und demnächst auch zwischen Arzt, Patient und technologischer Assistenz. Für ein Krankenhaus ergibt sich daher ein Dilemma: *Der Aufwand zum Umgang mit besonders schützenswerten Personendaten steht im Widerspruch zum Wunsch einer Nutzung dieser Daten im Sinne einer guten, gesundheitlichen Versorgung mit wirtschaftlicher Begründbarkeit; innerhalb und außerhalb des Krankenhauses*.

Die Ansprüche der Bevölkerung für eine gute Versorgung im Krankenhaus orientieren sich längst am Grad der Digitalisierung einer Einrichtung. Der einzelne Patient begründet seinen Anspruch an eine gute Versorgung noch selten mit dem Verweis auf die Qualität und Verfügbarkeit von Daten. Doch ihm vertraute Zusammenhänge im Umgang mit Daten allgemein, lassen ihn als Teilnehmer der digitalen Gesellschaft auf die Bedeutung schließen, ob und wie eine gesundheitliche Einrichtung Daten nutzt, um Genesung zu ermöglichen. Vor allem wo Daten einen sinnvollen, weil zielführenden Verlauf einer Krankheit bestimmen. Dabei lassen sich Patienten nicht mehr von einer falschen Nostalgie lenken, die einen Krankenhausaufenthalt romantischer erscheinen lässt.

Wo heute noch die unzureichende oder gar fehlende WLAN-Ausleuchtung Anlass bietet, den Komfort während eines Aufenthalts als Gast im Krankenhaus zu bewerten, überträgt sich Morgen eine anachronistische Handhabung im Umgang mit Daten auf die Bewertung neuer Qualitätskriterien, die ein Krankenhaus vorweisen werden muss. Der Patient sieht heute schon Indizien, die im engen Zusammengang mit dem Grad der Digitalisierung eines Krankenhauses stehen.

Und der Grad an Digitalisierung im Gesundheitswesen ist äußerst bescheiden, attestiert der Krankenhaus Rating Report 2018[7]. Der aktuell vorliegende Bericht verknüpft erstmals die Bewertungskriterien Personalknappheit in Krankenhäusern mit der Digitalisierung. Damit verliert die Digitalisierung im Krankenhaus ihren Nice-to-Have-Sta-

tus und avanciert zur Notwendigkeit im Rahmen der Ökonomisierungsbemühungen in der stationären Versorgung.

In den nächsten Jahren wird der Grad an Digitalisierung zum Wettbewerbsfaktor für Krankenhäuser, dem nicht mit steigenden Fallzahlen begegnet werden kann.

Beispiel klinische Patientenakte: Rund 2500 Krankenhäuser in Europa erreichen derzeit die beiden höchsten Technologiestufen nach dem international anerkannten Bewertungsmodell HIMSS: die papierlose elektronische Patientenakte, die alle klinischen Bereiche integriert und den Austausch mit anderen Leistungserbringern ermöglicht. In Deutschland sind es gerade zwei Kliniken, die diesen Status erreichen[8].

Ein Krankenhaus ist zunächst ein Unternehmen, wie jedes andere, das sich die Errungenschaften einer modernen Büro- und Prozessinfrastruktur erschließen muss. Analog zu Produktionsprozessen in einem Industrieunternehmen übernimmt die Datenverarbeitung in der Medizin immer wichtigere Aufgaben. Die Erbringung medizinischer Leistungen ist dabei nicht vergleichbar mit einem klassischen Produktionsprozess, der an smarte Maschinen delegiert werden kann. Auch wenn derartige Postulate im Raum stehen, die künstliche Intelligenz verdränge den Arzt langfristig. An ein solches Szenario ist in den nächsten Jahrzehnten im Krankenhaus nicht zu denken. Schon weil die Kompensation von Krankheit immer auch eine Co-Creation zwischen Patient und ärztlicher Kunst bleibt. Zwar wird die Unterstützung durch Assistenzsysteme deutlich zunehmen. An die angestrebte Automatisierung wie beispielsweise in Teslas Gigafactories ist dabei nicht zu denken und wäre auch aus ethischen Erwägungen nicht wünschenswert.

Trotzdem: Der Umgang mit Daten erfährt auch im Krankenhaus eine umfassende Neubewertung. Die Art und Weise des Umgangs mit medizinischen Daten im Krankenhaus wird zum Wettbewerbsfaktor und bestimmt damit die Zukunftsfähigkeit eines Krankenhauses. Digitale Daten dienen nicht mehr ausschließlich Abrechnungs- oder Dokumentationszwecken, sondern sind essentieller Teil der Leistungserbringung. Daten bestimmen künftig die Qualität und Sicherheit der Versorgung.

Anmerkungen

Fn. 7 | Vgl. Augurzky, B., Krolop, S. et al. (2018) Krankenhaus Rating Report 2018 Personal-Krankenhäuser zwischen Wunsch und Wirklichkeit. medhochzwei Verlag.

Fn. 8 | Vgl. Telgheder, M. (2018) Kliniken: Krankenhäusern fehlen bald Zehntausende Fachkräfte, handelsblatt.com.
Available at: https://www.handelsblatt.com/unternehmen/dienstleister/krankenhaus-rating-report-deutschen-kliniken-fehlen-bald-zehntausende-fachkraefte/22655736.html?ticket=ST-2543456-IssKimNqbSVA2TsMlqYq-ap2 (Accessed: 4 September 2018).

VII. Auswirkungen auf das Geschäftsmodell von Krankenhäusern

Auf diese Herausforderungen muss sich das Geschäftsmodell von Krankenhäusern einstellen. IT-Szenarien sind heute bereits Teil der Leistungserbringung. Doch aus einer dienenden Disziplin zur Sicherstellung des flankierenden Betriebs von medizintechnischen Hardware-Infrastrukturen und Software Architekturen entwickelt sich ein neuer zentraler Einfluss für die moderne Medizin, die auch das Krankenhaus betrifft. Das Krankenhaus als Plattform ist keine Utopie mehr.

Um den Status als spezialärztliche Institution zu erhalten, müssen sich Krankenhäuser einen neuen Umgang mit Gesundheitsdaten erschließen. In Anbetracht der finanziellen und operativen IT-Probleme unter denen viele Krankenhäuser leiden, mag das Szenario utopisch klingen. Doch ist bereits absehbar, das der systeminherante Schutzfaktor, der sich aus der besonderen Bedeutung ergibt, der Krankenhäusern im Gesundheitswesen zugestanden bleibt, ein anderer werden wird. Das oben angesprochene, exponentielle Wachstum an Datenmengen steht in enger Verbindung mit zur Verfügung stehenden Rechenkapazitäten, die eine bereits eingesetzte Entwicklung beschleunigen wird.

Schon heute fließen medizinische Leistungen kaskadenartig vom stationären in den ambulanten Sektor ab. Der ambulante Sektor wird konfrontiert mit Diagnosen und Therapien aus dem Netz. Der Alltag der Menschen wird zum Gesundheitssektor in dem sich neue Player und kleine Startups tummeln, die das hier postulierte neue Verständnis für eine datengetriebene Medizin bereits pflegen. Krankenhäuser und Ärzte werden auch zukünftig gebraucht. Geschäftsmodell und Berufsbild werden auf diese Entwicklungen mit geeigneten Strategien reagieren müssen. Eine Herausforderung ist der Umgang mit Gesundheitsdaten.

Anzuraten ist Krankenhäusern der digitalen Medizin mehr Platz in der Wertschöpfungskette zu bieten. Datengetriebene Medizin gilt gesellschaftlich als vereinbart. Sie kommt. Krankenhäuser die sich diesem Gedanken nicht anschließen, werden ausgeschlossen. Die Wahrscheinlichkeit, dass in Zukunft medizinische Leistungen wegfallen ist kurzfristig klein. Leistungen, die delegiert oder substituiert werden schon wahrscheinlicher. Die Assistenz z.B. durch eine künstliche Intelligenz ist dagegen schon Wirklichkeit. In jedem Fall befindet sich das Krankenhaus schon bald im Preiskampf und den wird es mit anachronistischen Szenerien gegenüber der datengetriebenen Medizin verlieren. Daher sollten Krankenhäuser Tech-Expertise aufbauen, den Zugang zum Kunden auch mittels Daten neu denken und Ihre Investitionen dahingehend anpassen.

In einem ersten Schritt bezieht sich das auf die neuen Tugenden für den Datenaustausch zwischen Krankenhaus, seinen Ärzten und Patienten. Wichtig bleibt auch, den einrichtungsübergreifenden Informationsfluss zwischen Ärzten selbst in die Hand zu nehmen und nicht darauf zu warten, was der Staat dahingehend unternimmt oder eben nicht.

Was den Teil des Informationsaustauschs von Gesundheitsdaten betrifft, erfährt der Patient dieser Tage durch die Projekte für Gesundheitsakten nach §68 SGB V eine autonomere Rolle, die ihn nicht mehr aussperrt.

VIII. Plädoyer für Ökonomisierung von Gesundheit durch Digitalisierung

Wann wird es endlich eine eigene Fallpauschale für Medienbrüche geben?

Es dürfte sich herumgesprochen haben, dass die Digitalisierung Hand in Hand geht mit dem Wunsch, die Gesundheitssysteme - und zwar weltweit - kostengünstiger zu gestalten. Damit verbunden ist der Wunsch, Dingen, die bislang ein physisches Dasein hatten, auf eine technologische Ebene zu heben. Das hat tatsächlich Potenzial, Dinge zu entstofflichen. Zum Beispiel Faxgeräte oder die Kurve, die früher noch am Krankenbett des Patienten hing, um darauf seine Gesundheitsdaten zu notieren. Man wusste, wo es war. Außerhalb der Visite, waren diese Gesundheitsdaten nicht nutzbar.

Abgesehen vom Menschen selbst steht Gesundheit als Wert nicht im Verdacht stofflich zu sein. Gesundheitsdienstleistungen sind - wie der Name schon sagt - Services und die werden - wo die Automatisierung fehlt - von Menschen erbracht. Das geflogene Wort, alles was sich digitalisieren lässt, wird digitalisiert, klingt da wie eine Mär. Was aber, wie oben angedeutet, wenn Dienstleistungen, wie wir sie heute im Leistungskatalog kennen, einfach verschwinden oder im Rahmen der Wertschöpfungskette zur Kompensation von Krankheit anders angesiedelt werden oder nicht mehr von Krankenhäusern erbracht werden?

Es gehört fast schon zum guten Ton, als Akteur im Gesundheitswesen nach mehr Geld zu rufen. Wird tatsächlich Geld freigegeben oder eine Umverteilung im System arrangiert, werden die neuen Mittel oft unmittelbar als Gesundheitsausgaben verbucht. Aufgeschobene Investitionen fließen in infrastrukturelle Maßnahmen oder in eine verbesserte Medizintechnik, um im Wettbewerb der Spezialisierungen Schritt zu halten.

Nicht nur im stationären Betrieb treiben diese Entwicklungen seit Jahren die Gesundheitskosten pro Kopf in die Höhe. Insgesamt wurde die Schallmauer von 1 Milliarde EUR für Gesundheitsausgaben pro Tag bereits durchbrochen. Bei Krankenhäusern liegt die Steigerungsrate für direkte Gesundheitsausgaben bei einer Steigerung von mehr als 3 Milliarden EUR pro Jahr seit 2013[9]. Die Gründe für diese Kostenexplosion sind vielfältig. Berechnungen versprechen eine partizipatorische Beteiligung am Wachstum durch die Demographie und um diese Marktanteile wird unter Krankenhäusern erbittert gekämpft. Im Wettbewerb um die beste Medizin sehen viele Experten zudem die Lösung, um Krankenhäuser, die in Leistung und Qualität und Zukunftsfähigkeit schlecht performen, vom Netz zu nehmen.

Einer ganz anderer Grund hängt aber in der Stellschraube für administrative Kosten rund um die gesundheitliche Versorgung der Bevölkerung. Der Wunsch nach einem höheren Digitalisierungsgrad in Krankenhäusern erfährt auch aus diesem Grund keine Priorität, scheint es doch so, als ob die Digitalisierung zunächst einen Teil des Gel-

des, das für die Versorgung der Kranken und eine bessere Medizin genutzt werden sollte, in der Administration verschwindet. Diese Schlussfolgerung könnte in Anbetracht dessen, dass wir die effiziente Nutzung von Gesundheitsdaten tatsächlich erreichen, falsch sein. Denn obwohl im ersten Schritt administrative Prozesse durch die Digitalisierung vereinfacht würden, um mittelfristig Kosten zu sparen, ist langfristig zu berücksichtigen, dass Menschen durch die Errungenschaften einer Digitalisierung des Gesundheitsgeschehens profitieren, weil sie gesünder leben, Krankheiten besser vorhergesagt werden oder gar ganz vermieden werden können. Allein die Ausgaben durch ein versagen der Arzneimitteltherapiesicherheit aufgrund fehlender Informationsflüsse reichen in die Millionen EUR.

Ein Paradigmenwechsel, hervorgerufen durch die Digitalisierung widerspricht so dem Geschäftsmodell eines Krankenhauses heute. Auch deshalb sind Veränderungen vor allem in der stationären Versorgung nicht gewollt. Dabei wäre eine sinnvolle Umverteilung der Investitionen dringend angezeigt. Zahlen im internationalen Vergleich zeigen, was es bedeuten kann, der heutigen Logik weiter zu folgen.

Gesundheitskosten steigen durch Investitionen in tradierte Paradigmen

Bei der Lebenserwartung seiner Bevölkerung lagen die USA im internationalen Vergleich noch nie auf einer Toplatzierung und seit Mitte der achtziger Jahre erhöhen sich die administrativen Gesundheitskosten pro Kopf rasant. Auch Deutschland weist in der nachfolgenden Abbildung hohe Kosten pro Kopf aus, liegt bei der Lebenserwartung aber deutlich vor den USA.

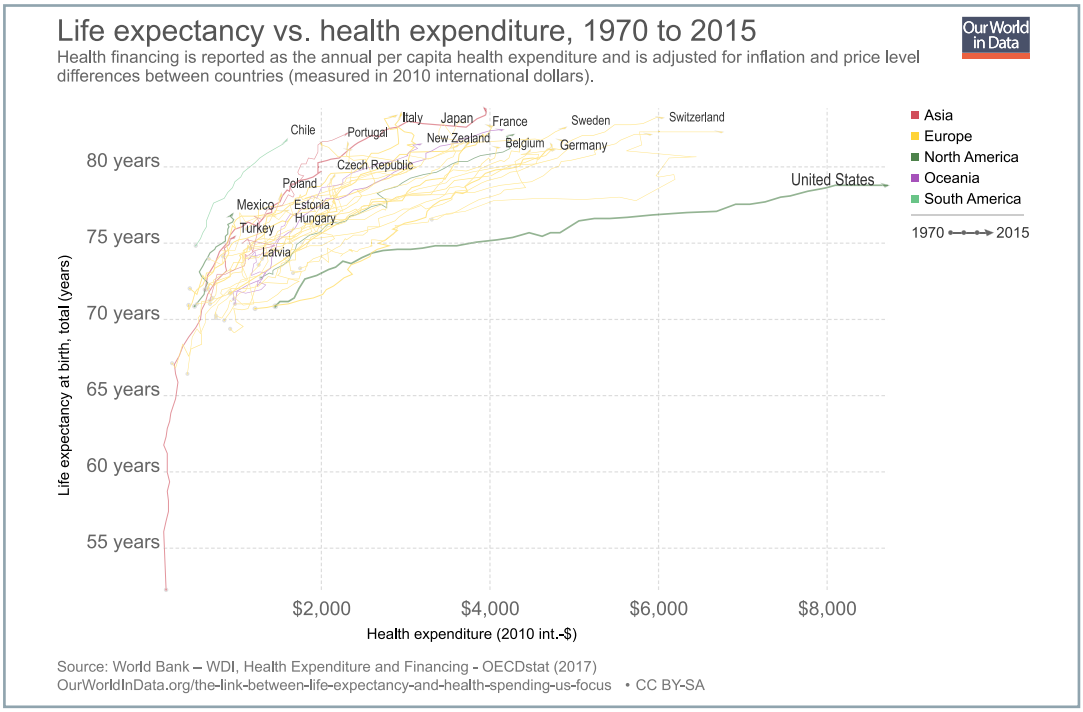


Abb. 2 Life expectancy vs. health expenditure, 1970 to 2015

Lebenserwartung| Die Lebenserwartung gibt an, wie alt ein Neugeborenes voraussichtlich werden wird, wenn sich die Sterblichkeitsrate zum Zeitpunkt seiner Geburt im Lauf seines Lebens nicht verändert.

Gesundheitsausgaben| Pro-Kopf-Kosten der Gesundheitsversorgung und ihrer Finanzierung in den OECD-Ländern, angegeben in internationalen Dollar (2010).

Für die USA ist außerdem zu berücksichtigen, dass die Schere bei den Ausgaben weit auseinander geht. Gerade einmal 5% der Bevölkerung wendet rund die Hälfte der gesamten Gesundheitskosten auf. Hinzu kommen die Systemunterschiede zwischen Europa und den USA. In Deutschland greift das Solidaritätsprinzip der allgemeinen Versicherungspflicht.

Trotzdem zeigt die Korrelation zwischen Lebenserwartung und die Ausgaben für Gesundheit pro Jahr einen eklatanten Unterschied zwischen Europa und den USA. Die Vereinigten Staaten zeigen eindrucksvoll, wie immer höhere Gesundheitskosten nach dem alten Paradigma in eine Sackgasse führen. Auch wenn die USA als Vorreiter in der Digitalisierung gelten und der zweite Gesundheitsmarkt dort deutlich größer sein dürfte. Die Errungenschaften der Projekte für digitale Gesundheit (Digital Health) sind in diesen Berechnungen noch nicht relevant. Argumentationen, die die hohen Kosten aufgrund des steigenden Grads an Digitalisierung anführen, sind ungültig, Die Gesundheitsausgaben in den USA steigen nicht wegen der Digitalisierung, sondern trotz der Digitalisierung.

Interessant in diesem Zusammenhang ist ein Projektbericht der Stiftung Münch. Darin heißt es: Das US Gesundheitssystem wird häufig aufgrund seiner bestenfalls durchschnittlichen Qualität bei zugleich hohen Kosten kritisiert. Dennoch lohnt sich ein differenzierter Blick. Die aus der starken Fragmentierung des Systems entstehenden Probleme eröffnen zahlreiche Ansatzpunkte für Experimente mit neuen Versorgungs- und Vergütungsformen. Zugleich treffen viele der in den USA vorliegenden Probleme auch auf Deutschland zu: Kostendruck, Brüche in der Kontinuität der Versorgung, Qualitätsdefizite, die Gefahr impliziter Rationierung, unzureichende IT-Infrastruktur, um nur einige zu nennen[10].

Die Schlussfolgerung kann daher nur lauten, den Trend für die administrativen Kosten möglichst schnell zu korrigieren und die digitale Gesundheit im Geschäftsmodell Krankenhaus zu berücksichtigen. Zum Beispiel, wenn sich durch die Digitalisierung des Gesundheitsgeschehens Krankenhausaufenthalte nach heutigem Vorbild langfristig nach unten korrigieren und das Krankenhaus der Zukunft seinen Platz in der Netzökonomie einnimmt.

Das setzt allerdings ein neues Verständnis und eine Kultur für Daten in der stationären Versorgung voraus, wie wir es heute noch nicht kennen. Daraus resultieren künftige Aufgabenstellungen einer Health-IT im Krankenhaus.

Anmerkungen

Fn. 9 | Vgl. Gesundheitsausgaben nach Einrichtungen - Statistisches Bundesamt (Destatis) destatis. Available at: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Gesundheit/Gesundheitsausgaben/Tabellen/Einrichtungen.html (Accessed: 4 September 2018).

Fn. 10 | Vgl. Netzwerkmedizin - Impulse für Deutschland aus den USA (2015). Available at: https://www.stiftung-muench.org/wp-content/uploads/2016/06/StudieUSA.pdf (Accessed: 4 September 2018).

Abb. 2 | Vgl. https://ourworldindata.org/the-link-between-life-expectancy-and-health-spending-us-focus

IX. Nutzen und Anspruch bei der Übertragung von Gesundheitsdaten

Mit Projekte wie Vivy greifen Patienten auf einen durch Krankenkassen getriebenen Service zurück, jedwede Daten über einen Krankenhausaufenthalt anzufordern, egal wann dieser stattgefunden hat. Korrelierend mit den Aufbewahrungsfristen halten Patienten damit ein Instrument in den Händen, Krankenhäuser auf Trab zu halten, Gesundheitsdaten bereitzustellen.

Zu unterscheiden ist hier zwischen Nutzen und Anspruch. Während der Nutzen in einer zeitnahen Anforderung von Gesundheitsdaten nach einem Krankenhausaufenthalt nachvollziehbar erscheint, kann auch ein allgemeiner Anspruch an den Daten entstehen, der teils auf Jahre zurückliegende Fälle zielt.

Die gesetzliche Lage zeigt, dass innerhalb der Fristen von für die Aufbewahrung Patienten Ihr Recht mit den durch die Krankenkassen forcierten Projekte unter Berücksichtigung von §68 SGB V in Anspruch nehmen könnten, was einen enormen Arbeitsaufwand erzeugen kann, wenn Krankenhäuser hier nicht vorbereitet sind oder gar durch eine Verweigerung zur Herausgabe in rechtliche Streitigkeiten verstrickt werden könnten.

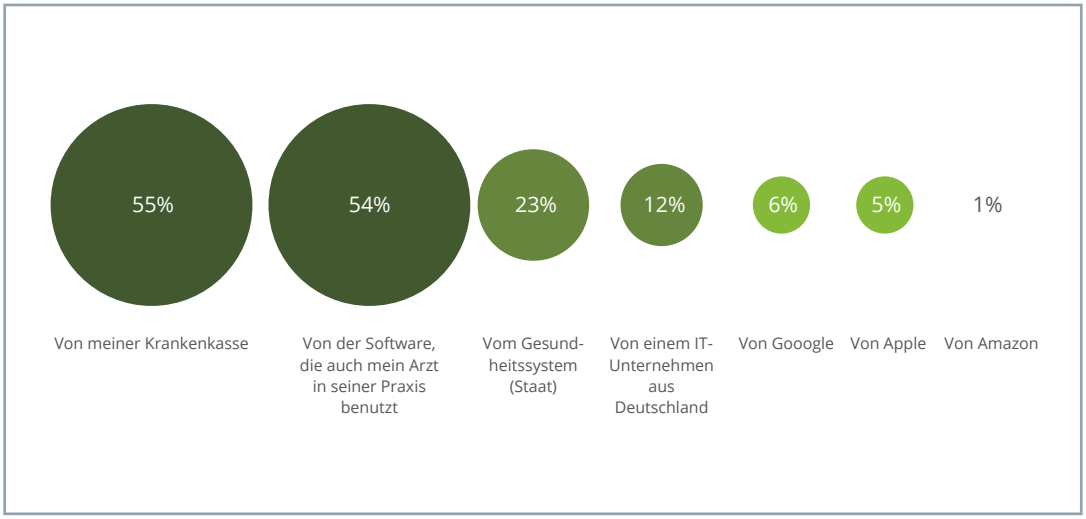
X. Akzeptanz der elektronischen Patientenakte

Einrichtungsübergreifende Elektronische Patientenakten oder auch Gesundheitsakten werden seit etwa 1990 als Instrument einer besseren Gesundheitsversorgung diskutiert[11].

In Deutschland wurde mit der elektronischen Gesundheitskarte (eGK) eine solche Akte in Aussicht gestellt. Die gegenseitige Blockierung der am Projekt Beteiligten, führte letztendlich dazu, dass über 2 Milliarden an Kosten entstanden, ohne dass bis heute eine elektronische Patientenakte vorliegt. Für 2021 wurde jetzt eine solche Akte in Verbindung mit der Telematikinfrastruktur angekündigt. Geht es nach Bundesgesundheitsminister Jens Spahn wird die Akte - in die Leistungserbringer die Daten Ihrer Patienten einspielen können - technisch überarbeitet und mobil zugänglich gemacht. Derzeit würde ein nur sehr umständliches Verfahren einen mobilen Zugang ermöglichen[12]. Faktisch entspricht die nicht dem Empfinden einer Benutzerfreundlichkeit der für diesen Fall breiten Gemeinschaft aus Bürgern, Versicherten und Patienten. Um die eGK mit einem Smartphone oder Tablet zu nutzen, muss ein Karten-Lesegerät über Bluetooth oder USB-Schnittstelle verbunden werden. Allein die Anschaffung eines Karten-Lesegeräts dürfte die eGK Inhaber abschrecken, bringen moderne Endgeräte doch kontaktlose Schnittstellen wie NFC mit[13].

Zudem befindet sich auch die Bevölkerung in einem Transformationsprozess. 58 Prozent der Befragten des ePatient Survey 2018 können anfänglich mit dem Begriff Online-Gesundheitsakte nichts anfangen, auf die Frage, ob sie digital jederzeit auf ihre Krankheitsdaten zugreifen wollen, antworten jedoch 73 Prozent mit Ja[14].

Abb. 3 Grafik: Anbieter, von denen Bürger und Patienten ihre Online-Gesundheitsakte haben wollen



Die Menschen in Deutschland haben eine klare Vorstellung mit welchem Akteur und über welche Kanäle sie ihre persönlichen Krankheitsdaten teilen wollen. Dabei spielt der mögliche Betreiber einer OnlineGesundheitsakte wie auch der direkte Ansprechpartner hierzu eine Rolle. Primär werden die behandelnden Ärzte und Kliniken bevorzugt. Entsprechend wollen Bürger und Patienten ihre Daten auch mit diesen Ansprechpartnern für eine bessere Therapie teilen[15].

Anmerkungen

Fn. 11 | Vgl. Haas, P. (2017) 'Elektronische Patientenakten: Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen', p. 288. doi: 10.11586/2017018.

Fn. 12 | Vgl. Borchers, D. (2017) Gematik: Elektronische Gesundheitskarte kann mobil genutzt werden – aber sehr umständlich | heise online, heise.de.
Available at: https://www.heise.de/newsticker/meldung/Gematik-Elektronische-Gesundheitskarte-kann-mobil-genutzt-werden-aber-sehr-umstaendlich-3700085.html (Accessed: 6 September 2018).

Fn. 13 | Vgl. Stratmann, F. (2017) eGK geht online - Die Party bleibt aus, XING News.
Available at: https://www.xing.com/news/insiders/articles/egk-geht-online-die-party-bleibt-aus-761159 (Accessed: 6 September 2018).

Fn. 14 - 15| Vgl. Schachinger, A. (2018) ePatient Survey 2018 Pressemappe.
Available at: https://www.epatient-rsd.com/survey/ (Accessed: 6 September 2018).

Abb. 3 | Vgl. https://www.epatient-rsd.com/aktuelles/

Fazit

Die Speicherung von Gesundheitsdaten wird eher dezentraler als zentraler. Projekte zur Speicherung von Gesundheitsdaten orientieren sich derzeit am Anspruch der Patienten, Zugriff auf die Patientendaten zu haben. Diese einrichtungsübergreifenden Aktenprojekte spielen zunehmend eine Rolle im Alltag des Krankenhauses. Zumal zu erwarten bleibt, dass sich diese Projekte zu echten Gesundheitsplattformen weiterentwickeln.

Durch eine sich verändernden Kultur im Umgang mit Gesundheitsdaten stehen Krankenhäuser vor der Herausforderung, ihre Geschäftsmodelle anzupassen, die derzeit stark von politischen Entscheidungen geprägt sind und der Rolle, die ihnen das Gesundheitswesen zugesteht.

Die datengetriebene, digitale Medizin macht Boden gut und stellt den Status Quo der Krankenhäuser in Frage. Langsam aber stetig verändert sich die gesundheitliche Versorgung. Wollen Krankenhäuser nicht zum reinen Reparaturbetrieb degradiert werden, müssen sie sich verändern und zumindest in Teilen damit beginnen, sich der datengestützten Medizin zuzuwenden.

Die Medizin der Zukunft wird bestimmt von der Digitalisierung. Sie wird im Umgang mit Gesundheitsdaten Anschluss halten müssen. Und zwar zum Wohle der Patienten. Bei aller Euphorie. Die neue, datengetriebene Medizin muss auch im Krankenhaus weiterhin Heilung fördern und durch Zuwendung und Empathie begleitet werden. Der Innovationssprung durch die auftauchenden neuen Player überträgt sich auf die Medizin als Herausforderungen im Krankenhaus. Und dieser Sprung steht unmittelbar bevor. Die Nutzung und Interpretation von digitalen Daten wird die medizinische Versorgung grundlegend verändern und neue Möglichkeiten eröffnen – von der Anamnese über die Diagnose bis hin zur Therapie[16].

Anmerkungen

Fn. 16 | Vgl. Werner, J. (2016) Smart Hospital Auf dem Weg zum Krankenhaus der Zukunft. Jahresbericht des Universitätsklinikums Essen, das sich zum digitalsten Krankenhaus der Welt entwickeln will.

Teil 2

Datensicherheit für elektronische Patientenakten

Zusammenfassung

Kaum eine andere Branche ist so stark reguliert wie das Gesundheitswesen, und das aus gutem Grund: Die Integrität persönlicher Gesundheitsinformationen (Personal Health Information, PHI) ist für die erfolgreiche Behandlung von Patienten von entscheidender Bedeutung. Darüber hinaus erfassen und speichern Unternehmen und Organisationen im Gesundheitswesen nicht nur Gesundheitsinformationen, sondern auch eine Vielzahl anderer personenbezogener Daten. Da sowohl persönliche Gesundheitsinformationen als auch personenbezogene Daten für Akteure auf dem Schattenmarkt einen hohen Wert besitzen, sind Arztpraxen, Krankenhäuser und andere medizinische Einrichtungen ein attraktives Ziel für Cyberangriffe.

Entsprechend genießt das Thema Datensicherheit für die IT-Abteilungen vieler dieser Einrichtungen und ihrer Geschäftspartner höchste Priorität. Die Zahl der Datenschutzverletzungen im Gesundheitswesen zeigt jedoch, dass es dringend besserer Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von elektronischen Patientenakten (ePA) bedarf.

Die Plattform *Netwrix Auditor* bietet Transparenz und Governance für zuverlässige Sicherheit in Hybrid-Cloud-Umgebungen. Sie wird weltweit bereits von mehr als 630 Unternehmen im Gesundheitswesen eingesetzt, um Risiken für sensible Daten einzudämmen und gesetzlich vorgeschriebene Audits erfolgreich zu bestehen. Auch Sie können von diesen Vorteilen profitieren.

Dieses E-Book beschreibt ausführlich, wie sich Unternehmen im Gesundheitswesen mit Netwrix Auditor besser vor Cyberbedrohungen und damit vor Gefahren für *hochgradig sensible persönliche Gesundheitsinformationen* schützen können. Sie finden darin außerdem Empfehlungen, wie Sie sich auf gesetzlich vorgeschriebene Compliance-Audits vorbereiten und diese erfolgreich bestehen. Sie erhalten Antworten auf alle wichtigen Fragen:

- Wie können Sie sich besser vor Cyberbedrohungen schützen, die eine Gefahr für Ihre hochgradig sensiblen persönlichen Gesundheitsinformationen darstellen?
- Wie können Sie Schwachstellen in in Ihren Sicherheitssystemen und -maßnahmen aufdecken und Angriffe frühzeitig erkennen?
- Wie können Sie die Rechenschaftspflicht des Einzelnen sicherstellen und Richtlinienverstößen vorbeugen?
- Wie können Sie sich effektiver auf Compliance-Audits vorbereiten und diese erfolgreich bestehen?

I. Proaktive Erkennung von Vorfällen, die eine Gefahr für Gesundheitsinformationen darstellen

Da wir geschützte Gesundheitsinformationen verarbeiten, sind Vertraulichkeit und Integrität für uns unabdingbar. Vor der Implementierung von Netwrix Auditor hatten wir nicht annähernd den gewünschten Einblick in Änderungen an unserem SQL-Server und Zugriffe auf sensible Daten. Mit Netwrix Auditor verfügen wir über umfassende Transparenz im Hinblick auf Änderungen am SQL-Server bis hinab auf die Ebene einzelner Spalten und Zeilen der Datenbank. Unser früheres System bot lediglich punktuelle Einblicke.

Accretive Health

Ein wichtiger erster Schritt für einen besseren Schutz von Patientendaten ist die Kontrolle von Benutzer- und Computerkonten, Benutzergruppen und Berechtigungen unter Einhaltung von modernen Best Practices für die Sicherheit. Ein klar strukturiertes Benutzer- und Berechtigungsmanagement schmälert das Risiko eines versehentlichen unerlaubten Zugriffs auf sensible Daten, begrenzt den Schaden bei vorsätzlichen Verstößen und ermöglicht eine rechtzeitige Erkennung von Angriffen.

Sie benötigen außerdem geeignete Überwachungsfunktionen, um Anzeichen für unzulässige oder in sonstiger Weise verdächtige Aktivitäten, die Ihre ePA gefährden könnten, rechtzeitig zu erkennen. Hierzu müssen Sie in der Lage sein, sämtliche Aktivitäten in Ihrer IT-Infrastruktur zu erfassen, schnell zwischen wichtigen und unwichtigen Ereignissen zu unterscheiden und Informationen zueinander in Bezug zu setzen. So ergibt sich ein Gesamtbild, das es Ihnen ermöglicht, sowohl bereits erfolgte Angriffe als auch mögliche Angriffsflächen zu identifizieren.

Mit Netwrix Auditor haben Sie stets den Überblick über alle Konten, Gruppen und Berechtigungen und können sämtliche Änderungen überwachen, um möglichen Sicherheitslücken vorzubeugen. Sie profitieren damit außerdem von umfassenden Berichtsfunktionen, die die Erkennung vorhandener und potenzieller Bedrohungen deutlich vereinfachen.

Vermeidung unnötiger Risiken durch Kontrolle von Benutzer- und Computerkonten

Eine unzureichende Kontrolle über Benutzer- und Computerkonten ist der erste Punkt, an dem Sie ansetzen sollten, damit die komplexen Bedrohungen von heute möglichst keine Gefahr für Ihre sensiblen Daten (z. B. Patientenakten) darstellen. Netwrix Auditor ermöglicht eine einfache Überprüfung der Integrität von Konten und sorgt durch eine schnelle Problembehebung für mehr Sicherheit. Vordefinierte Berichte geben Aufschluss über die Gesamtzahl aller Konten und enthalten auch wichtige Informationen, unter anderem zum Pfad, Status oder Zeitpunkt der letzten Anmeldung. Anhand historischer Snapshots können Sie außerdem den Status von Benutzerkonten zu einem beliebigen Zeitpunkt überprüfen.

Abb. 4 Bildschirm »User Accounts«

Zeigt Benutzerkonten, die dazugehörigen Pfade, Anmeldenamen, Statusinformationen (aktiviert oder deaktiviert) und den Zeitpunkt der letzten Anmeldung an.

User Accounts

Shows user accounts, their paths, logon names, statuses (enabled or disabled), and last logon time.

Total Enabled: 9
Total Disabled: 23
Total Count: 32

Path	Name	Logon Name	Status	When
\com\enterprise \Inactive Users\Alex Terry	Alex Terry	A.Terry	Disabled	23/10/2016 7:56:44 AM
\com\enterprise \Users\Anna Watson	Anna Watson	A.Watson	Enabled	28/11/2016 10:12:32 AM
\com\enterprise \Users\Administrator	Administrator	Administrator	Disabled	30/09/2016 11:05:17 AM

Netwrix Auditor ermöglicht zudem eine schnelle Suche und Analyse aller inaktiven, gesperrten und abgelaufenen Konten. Mithilfe der Plattform können Sie auch den potenziellen Missbrauch von Konten und Richtlinienverstöße aufdecken. Hierzu stehen Ihnen Berichte zu temporären Benutzerkonten (»Temporary User Accounts«), zu temporären Benutzern in privilegierten Gruppen (»Temporary Users in Privileged Groups«), zu kürzlich aktivierten Konten (»Recently Enabled Accounts«) und viele andere zur Verfügung.

Abb. 5 Bildschirm »Inactive Users in Active Directory Report«

Zeigt die inaktiven Konten an.

Inactive Users in Active Directory Report

The following accounts are no longer active:

Account Name	Account Type	E-Mail	Inactivity Time	Account Age
A.Kowalski	User	A.Kowalski@enterprise.com	33 day(s)	307 day(s)
S.Parker	User	S.Parker@enterprise.com	37 day(s)	311 day(s)
D.Lopez	User	D.Lopez@enterprise.com	40 day(s)	77 day(s)
R002312	User	None	21 day(s)	400 day(s)
T.Simpson	User	T.Simpson@enterprise.com	10 day(s)	255 day(s)

Gewährleistung des rechtmäßigen Zugriffs auf ePA durch Kontrolle der Gruppenzugehörigkeit

Eine weitere »goldene Regel« zum Schutz sensibler ePA besteht darin, die Zugehörigkeit von Benutzern zur richtigen Gruppe sicherzustellen. Es gibt durchaus legitime Gründe, die Gruppenzugehörigkeit zu ändern, beispielsweise wenn ein Mitarbeiter innerhalb des Unternehmens auf eine andere Position wechselt. Solche Änderungen können jedoch auch ein Hinweis auf den Versuch einer unbefugten Erweiterung von Benutzerrechten sein. Mit Netwrix Auditor können Sie Gruppenzugehörigkeiten ganz einfach routinemäßig prüfen und bestätigen, unter anderem mit Berichten zur tatsächlichen Gruppenzugehörigkeit (»Effective Group Membership«) oder zur Zugehörigkeit zur Administratorgruppe (»Administrative Group Members«).

Abb. 6 Bildschirm »Effective Group Membership«

Zeigt die Benutzer- und Computerkonten an, die einer bestimmten Gruppe angehören, sowie Statusinformationen (aktiviert oder deaktiviert) zu den einzelnen Konten. Sie können außerdem erkennen, ob ein Konto explizit zu einer Gruppe hinzugefügt wurde oder aufgrund der Gruppenzugehörigkeit implizites Mitglied der Gruppe ist.

Effective Group Membership

Lists user and computer accounts that belong to a specified group, the status (enabled, disabled) for each account, and whether the account was explicitly named as a member of the group or was included implicitly through group membership.

Name	Member Through	Type	Status
Administrator	Explicit	user	Disabled
Anna Kowalski	Explicit	user	Disabled
Anna Watson	Explicit	user	Enabled
Danny Johnson	Explicit	user	Enabled
Elena Anderson	Explicit	user	Enabled
Garry Brown	Explicit	user	Disabled
John Carter	Explicit	user	Enabled

Bestimmte Änderungen der Gruppenzugehörigkeit deuten darauf hin, dass die Sicherheit persönlicher Gesundheitsinformationen sehr wahrscheinlich gefährdet ist. Insbesondere ist es ungewöhnlich, wenn ein Benutzerkonto unmittelbar nach der Erstellung und dem Hinzufügen zu privilegierten Gruppen gelöscht wird. Es könnte sich dabei um einen Mitarbeiter mit betrügerischen Absichten oder eine externe Person handeln, die versucht, sich erweiterte Zugriffsrechte zu verschaffen und ihre Spuren zu verdecken. Mit Netwrix Auditor können Sie solche Bedrohungen mithilfe des Berichts zu temporären Benutzern in privilegierten Gruppen (»Temporary Users in Privileged Groups«) erkennen.

Abb. 7 Bildschirm »Temporary Users in Privileged Groups«

Zeigt die Benutzerkonten an, die kurz nach ihrer Erstellung und dem Hinzufügen zu privilegierten Gruppen (z. B. Domänen-Admins, Organisations-Admins, Schema-Admins, Konten-Operatoren und anderen Gruppen) wieder gelöscht wurden. Mithilfe dieses Berichts können Sie Eindringversuche mit böswilliger Absicht aufdecken.

Temporary Users in Privileged Groups

Shows user accounts deleted soon after they were created and added to privileged groups, such as Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other groups you specified. Use this report to detect intruders attempting to hide malicious activity.

Name	When Created	Who Created	When Removed	Who Removed
enterprise.com /Garry Smith	1/12/2016 1:27:58 AM	ENTERPRIS \J.Carter	1/12/2016 1:29:34 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				
enterprise.com /Richard Smith	1/12/2016 1:30:13 AM	ENTERPRIS \J.Carter	1/12/2016 1:32:42 AM	ENTERPRIS \J.Carter
Group Name: \com\enterprise\Users\Domain Admins				

Vermeidung unbefugter Berechtigungsausweitung und Datenextfiltration durch Kontrolle der Berechtigungen

Durch zu weit gefasste Zugriffsberechtigungen steigt das Risiko, dass Patientendaten offengelegt oder böswillig gelöscht werden. Mit Netwrix Auditor können Sie ein Konzept der geringsten Rechte umsetzen, das eine ordnungsgemäße Rollentrennung und das Zuweisen temporärer Berechtigungen ermöglicht, indem Sie ganz einfach Benutzer mit Berechtigungen anzeigen lassen können, die für ihre Rolle nicht relevant sind oder für bestimmte Aufgaben nicht benötigt werden.

Abb. 8 Bildschirm »Excessive Access Permissions«

Zeigt Konten mit Berechtigungen für Dateien und Ordner an, auf die selten zugegriffen wird. Mithilfe dieses Berichts können Sie überflüssige Berechtigungen ermitteln und Datenschutzverletzungen verhindern. Sie können untersuchen, welche Berechtigungen den Konten direkt zugewiesen oder aufgrund ihrer Gruppenzugehörigkeit erteilt wurden.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Patient History (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and list folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	0

Der Schutz von Systemen und Anwendungen mit sensiblen medizinischen Daten erfordert die regelmäßige Überprüfung, welche Kontoinhaber welche Berechtigungen besitzen. Mit Netwrix Auditor können Sie schnell und einfach erkennen, wer auf bestimmte Freigaben und Ordner mit sensiblen Daten zugreifen kann, welche Berechtigungen diese Benutzer haben und ob es sich dabei um geerbte oder explizit zugewiesene Berechtigungen handelt. Anhand historischer Snapshots können Sie die Berechtigungen eines Benutzers zu einem bestimmten Zeitpunkt in der Vergangenheit überprüfen und diese mit seinen gegenwärtigen Zugriffsrechten oder den von Ihnen definierten Standardberechtigungen vergleichen.

Abb. 9 Bildschirm »Object Permissions by Object«

Zeigt die Zugriffsberechtigungen für Dateien und Ordner nach Objektpfad gruppiert an, die einzelnen Konten (direkt oder aufgrund ihrer Gruppenzugehörigkeit) erteilt wurden. Anhand dieses Berichts können Sie erkennen, wer auf bestimmte Dateien und Ordner zugreifen kann. Sie können außerdem bestimmen, ob die Berechtigungen für ein Objekt mit den Berechtigungen für das übergeordnete Objekt übereinstimmen oder von diesen abweichen.

Object Permissions by Object

Shows file and folder permissions granted to accounts (either directly or via group membership), grouped by object path. Use this report to see who has access to files and folders, and determine whether the set of permissions on an object is the same or different from its parent.

Object: \\fs1\Shared (Permissions: Different from parent)

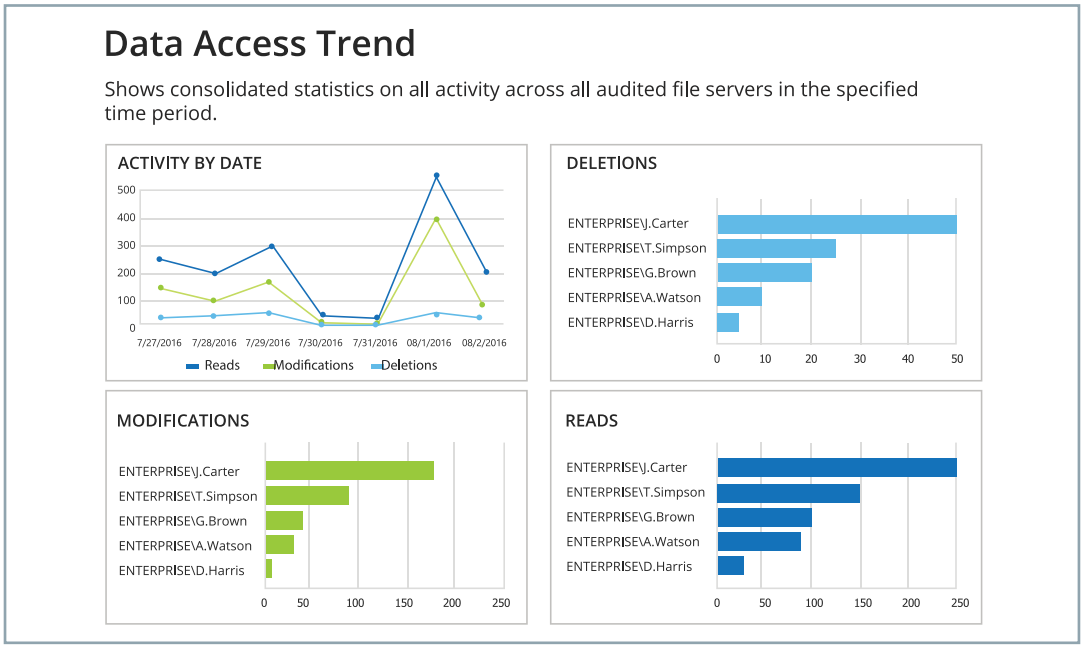
Account	Permissions	Means Granted
ENTERPRISE\A.Kowalski	Full Control	Group
ENTERPRISE\A.Watson	Full Control	Group
ENTERPRISE\Administrator	Full Control	Group
ENTERPRISE\G.Brown	Full Control	Group
ENTERPRISE\J.Carter	Read (Execute, List folder content)	Directly
ENTERPRISE\P.Anderson	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
fs1\Administrator	Full Control	Group

Schutz von Patientendaten durch sofortige Erkennung ungewöhnlicher Benutzeraktivitäten

Eine plötzliche Zunahme der Aktivitäten eines Benutzers, beispielsweise der Abruf zahlreicher Dateien oder eine große Zahl von Änderungen und Löschvorgängen, kann ein Hinweis darauf sein, dass die Sicherheit Ihrer persönlichen Gesundheitsinformationen gefährdet ist. Die Herausforderung besteht darin, diese kurzzeitige Zunahme von Aktivitäten stets im Blick zu behalten. Die Dashboards »Data Access Trend« und »File Servers Overview« von Netwrix Auditor halten Sie auf dem Laufenden, damit Sie Ihre Daten zuverlässig schützen können.

Abb. 10 Bildschirm »Data Access Trend«

Zeigt die Gesamtstatistik zu den Aktivitäten aller überwachten Dateiserver für den angegebenen Zeitraum an.



Auch auf die Löschung von Daten aus wichtigen Verzeichnissen, SQL- und Oracle-Datenbanken sowie SharePoint-Websites müssen Sie schnell reagieren können. Für einen zuverlässigen Schutz Ihrer persönlichen Gesundheitsinformationen ermöglichen die vordefinierten Berichte von Netwrix Auditor eine umgehende Erkennung dieser Bedrohungen. So können Sie die betroffenen Mitarbeiter oder das IT-Team benachrichtigen, das die Situation besser einschätzen kann. Andere Berichte geben Aufschluss darüber, welche Daten geändert oder neu hinzugefügt wurden. Auf diese Weise können Sie dafür sorgen, dass Patientenakten nicht außerhalb der dafür vorgesehenen Workflows verarbeitet werden.

Abb. 11 Bildschirm »Files and Folders Deleted«

Zeigt gelöschte Dateien und Ordner mit ihren Attributen an.

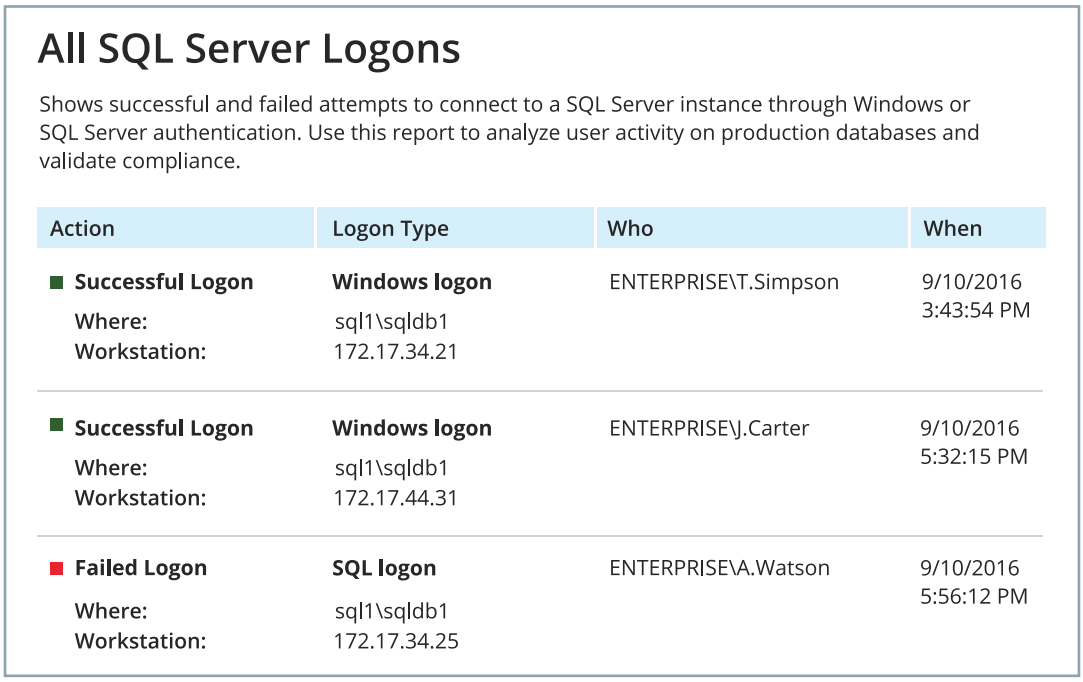
Files and Folders Deleted

Shows removed files and folders with their attributes.

Action	Object Type	What	Who	When
Removed	File	\\fs1\Out-patient \ClinicalRecords2016\J.Smith.rtf	ENTERPRISE\ J.Carter	7/18/2016 5:02:02 PM
Where:	fs1			
Removed	File	\\fs1\MaternityUnit\Births \T.Kelly.rtf	ENTERPRISE\ J.Carter	7/18/2016 5:02:03 PM
Where:	fs1			
Removed	File	\\fs1\Traumatology\Statistics \Report_spring_03.01.2016.xlsx	ENTERPRISE\ J.Carter	7/18/2016 5:02:04 PM
Where:	fs1			

Aufdeckung potenziell böswilliger Absichten durch Prüfen von Anmeldeaktivitäten

Durch eine sorgfältige Überprüfung von Anmeldeaktivitäten können Sie Gefahren für sensible Gesundheitsdaten aufdecken. Die Erfassung und Analyse dieser Informationen ist jedoch häufig mühsam und zeitaufwendig. Netwrix Auditor bietet Einblick in sämtliche Anmeldeaktivitäten auf den IT-Systemen in Ihrer Umgebung und vereinfacht damit die Überprüfung. Alle interaktiven und nicht interaktiven Anmeldungen werden überwacht und in Berichten erfasst – unabhängig davon, ob sie erfolgreich waren oder nicht. Zu jeder Anmeldung werden außerdem zusätzliche Detailinformationen gespeichert, die Sie später auswerten können, wenn Sie verdächtige Aktivitäten in Ihrem Netzwerk entdecken.



All SQL Server Logons

Shows successful and failed attempts to connect to a SQL Server instance through Windows or SQL Server authentication. Use this report to analyze user activity on production databases and validate compliance.

Action	Logon Type	Who	When
Successful Logon **Where:** **Workstation:**	**Windows logon** sql1\sqldb1 172.17.34.21	ENTERPRISE\T.Simpson	9/10/2016 3:43:54 PM
Successful Logon **Where:** **Workstation:**	**Windows logon** sql1\sqldb1 172.17.44.31	ENTERPRISE\J.Carter	9/10/2016 5:32:15 PM
Failed Logon **Where:** **Workstation:**	**SQL logon** sql1\sqldb1 172.17.34.25	ENTERPRISE\A.Watson	9/10/2016 5:56:12 PM

Abb. 12 Bildschirm »All SQL Server Logons«

Zeigt erfolgreiche und fehlgeschlagene Versuche an, über die Windows- oder SQL Server-Authentifizierung eine Verbindung zu einer SQL Server-Instanz herzustellen. Mithilfe dieses Berichts können Sie die Benutzeraktivitäten in den Datenbanken der Produktivumgebung analysieren und auf Compliance überprüfen.

Bestimmte Arten von Anmeldeereignissen erfordern eine permanente Überwachung. Insbesondere Anmeldungen zu ungewöhnlichen Zeiten, mehrfache Anmeldungen innerhalb eines kurzen Zeitraums, Anmeldungen über untypische Endgeräte und wiederholte erfolglose Anmeldeversuche sind Warnhinweise, die auf böswillige Insider-Aktivitäten, die Nutzung einer falschen Identität oder automatisierte Eindringversuche schließen lassen. Mit Netwrix Auditor können Sie Ereignisse dieser Art anhand von Berichten zu den Anmeldungen eines Benutzers über mehrere Endgeräte (»Logons by Single User from Multiple Endpoints«), den Anmeldungen mehrerer Benutzer über ein bestimmtes Endgerät (»Logons by Multiple Users from Single Endpoint«) oder auch zu den Konten mit den meisten Anmeldeaktivitäten (»Accounts with Most Logon Activity«) aufdecken.

Abb. 13 Bildschirm »Logons by Single User from Multiple Endpoints«

Zeigt die Benutzer an, die sich innerhalb kurzer Zeit über mehrere Endgeräte angemeldet haben. Solche Aktivitäten können ein Hinweis darauf sein, dass das Kennwort eines Kontos gestohlen oder kompromittiert wurde. Mithilfe dieses Berichts können Sie verdächtige Benutzeraktivitäten aufdecken und Datenschutzverletzungen verhindern.

Logons by Single User from Multiple Endpoints

Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the account's password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

User: ENTERPRISE\J.Carter (First Attempt: 7/27/2016 2:02:26 PM)

Endpoint	Logon Attempts
172.17.6.36	2
ENTWKS0376	6
WST055	12
192.168.1.1	1

Identifizierung von Richtlinienverstößen durch Analyse fehlgeschlagener Aktivitäten

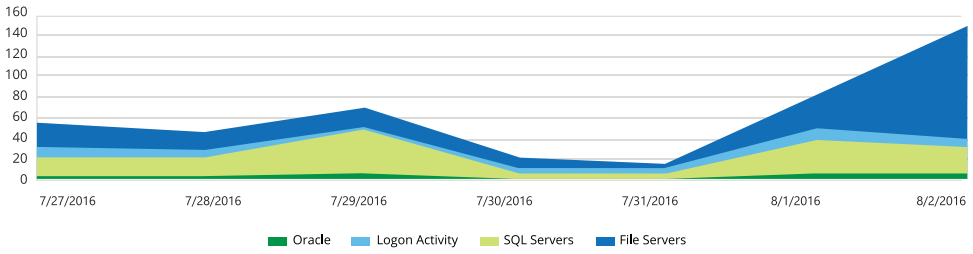
In jeder Umgebung führen alltägliche Fehler der Benutzer immer wieder dazu, dass das Abrufen, Ändern, Löschen oder Hinzufügen von Daten nicht funktioniert. Eine plötzliche Zunahme oder ein kontinuierlicher Anstieg solcher fehlgeschlagener Aktivitäten kann jedoch auch auf böswillige Versuche hinweisen, auf persönliche Gesundheitsinformationen zuzugreifen. Mit Netwrix Auditor können Sie bestimmen, bis zu welchem Umfang fehlgeschlagene Aktivitäten in Ihrem Unternehmen normal sind, und verdächtige Trends erkennen. Das Dashboard »Failed Activity Trend« enthält zudem eine Liste der Benutzer mit den meisten erfolglosen Versuchen. Sie können sich über dieses Dashboard weitere Details zu diesen Benutzern und ihren Aktionen anzeigen lassen.

Abb. 14 Bildschirm »Failed Activity Trend«

Zeigt die Gesamtstatistik zu fehlgeschlagenen Aktionen an, unter anderem Informationen zur Anzahl der erfolglosen Leseversuche, Änderungsversuche, Anmeldungen usw. Der Bericht führt außerdem die Benutzer mit den meisten erfolglosen Versuchen auf.

Failed Activity Trend

Shows consolidated statistics on failed actions, including failed read attempts, failed modification attempts, failed logons, etc. The report also lists the users with most failed attempts.



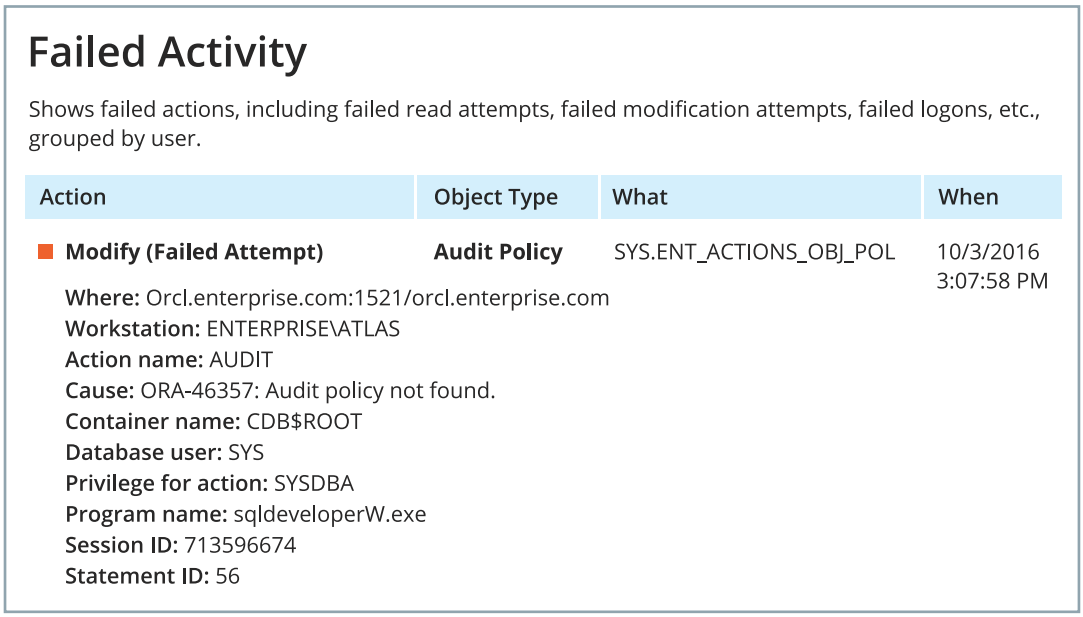
Date: 8/2/2016 (Attempts: 90)

Who	Attempts
ENTERPRISE\D.Harris	78
ENTERPRISE\G.Brown	7

Die umgehende Erkennung von erfolglosen Versuchen, Daten aus Ihren geschützten Datenbanken und von Netzwerklaufwerken abzurufen, zu ändern, zu kopieren oder zu löschen, ist besonders wichtig – denn genau hier werden sensible medizinische Informationen und personenbezogene Daten in der Regel gespeichert. Netwrix Auditor vereinfacht die Überprüfung fehlgeschlagener Aktivitäten in wichtigen Daten-Repositories wie Oracle-Datenbanken und Dateiservern und hilft Ihnen so, Ihre elektronisch gespeicherten persönlichen Gesundheitsinformationen zu schützen.

Abb. 15 Bildschirm »Failed Activity«

Zeigt fehlgeschlagene Aktionen nach Benutzern gruppiert an, unter anderem Informationen zur Anzahl erfolgloser Leseversuche, Änderungsversuche, Anmeldungen usw.



Failed Activity

Shows failed actions, including failed read attempts, failed modification attempts, failed logons, etc., grouped by user.

Action	Object Type	What	When
Modify (Failed Attempt)	**Audit Policy**	SYS.ENT_ACTIONS_OBJ_POL	10/3/2016 3:07:58 PM

Where: Orcl.enterprise.com:1521/orcl.enterprise.com
Workstation: ENTERPRISE\ATLAS
Action name: AUDIT
Cause: ORA-46357: Audit policy not found.
Container name: CDB$ROOT
Database user: SYS
Privilege for action: SYSDBA
Program name: sqldeveloperW.exe
Session ID: 713596674
Statement ID: 56

Anmerkungen

Abb. 4 - 15 | Abbildungsnachweis Netwrix Auditor 9.5

II. Optimierung von Untersuchungen durch unternehmensweite Transparenz

Wenn ein Problem auftritt, kann man die Ereignisprotokolle analysieren. Doch angesichts der Vielzahl der Einträge ist das so, als ob man nach einer Nadel im Heuhaufen sucht. Und oft findet man dabei noch nicht einmal die Daten, die man eigentlich benötigt. Mit Netwrix Auditor ist es wesentlich einfacher, eine solche Untersuchung durchzuführen und eine Antwort auf die Frage zu finden, warum etwas passiert.

Speare Memorial Hospital

Wie oben ausführlich erläutert, hilft Netwrix Auditor Ihnen durch das Aufspüren von Bedrohungen in Ihrer IT-Umgebung, Ihre sensiblen Gesundheitsinformationen zu schützen. Die Lösung kann jedoch noch mehr. Um zeitnah und effektiv auf eine Bedrohung oder einen Vorfall reagieren zu können, müssen Sie in der Lage sein, eine schnelle und zugleich gründliche Untersuchung durchzuführen und Benutzer für ihre Aktivitäten zur Rechenschaft zu ziehen. Sie müssen auch umfangreiche Prüfdaten einfach durchsuchen können, um die gewünschten Informationen zu finden. Diese Informationen müssen zuverlässig und konsistent sein, und alle Nachweise müssen sich so verknüpfen lassen, dass sie ein aussagekräftiges Gesamtbild ergeben.

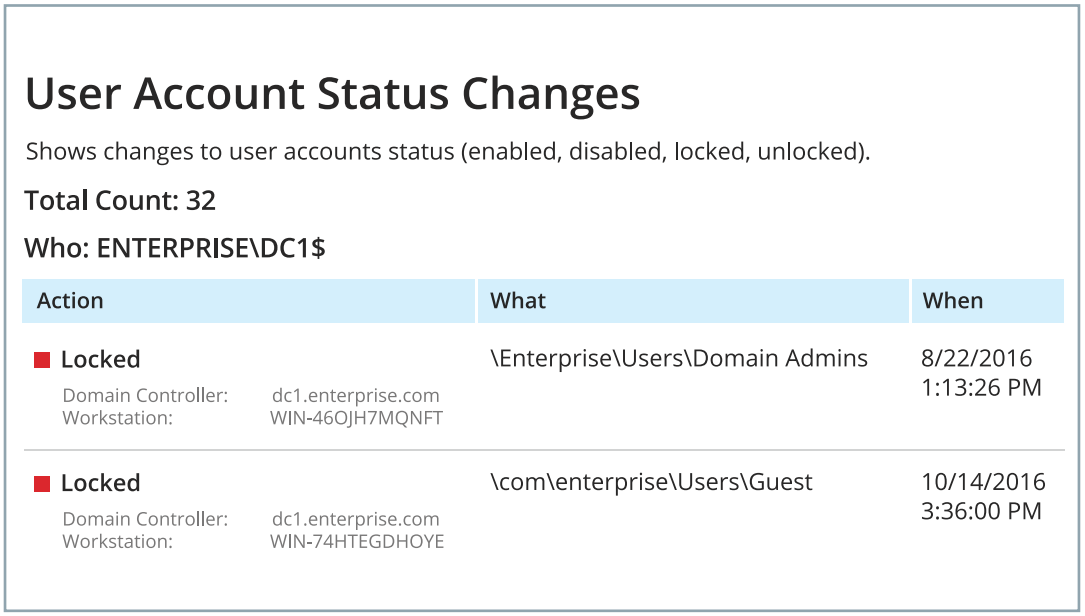
Netwrix Auditor ermöglicht eine effizientere Untersuchung potenzieller Sicherheitsverletzungen, indem umfangreiche Daten erfasst und so ausgewertet werden, dass Sie die nötigen Rückschlüsse ziehen können. Sie können beispielsweise Schritt für Schritt präzise nachvollziehen, welche Aktionen in Ihrer IT-Umgebung durchgeführt wurden, und durch die Rekonstruktion von Ereignissen mit allen relevanten Kontextinformationen feststellen, ob es sich bei einem Problem um einen böswilligen Angriff oder einen einfachen Fehler handelt. Mit Netwrix Auditor können Sie umgehend auf Vorfälle reagieren, Sicherheitsrichtlinien durchsetzen und Benutzer für ihre Aktionen zur Rechenschaft ziehen.

Identifizierung von Richtlinienverstößen durch Analyse fehlgeschlagener Aktivitäten

Allzu oft passiert es, dass es für das IT-Team aufgrund von Blind Spots und eingeschränkter Transparenz schwierig ist, die Geschehnisse bei einem Sicherheitsvorfall lückenlos nachzuvollziehen. Netwrix Auditor stellt vordefinierte Berichte mit vielen wertvollen Detailinformationen bereit, die umfassende Nachweise liefern, wer was wann und wo getan hat. Sie können sich mit diesen Berichten gezielt Informationen zu einem bestimmten Benutzer, einem bestimmten System, einer bestimmten Aktivität oder auch Details zu allen Aktivitäten auf einer Vielzahl von Systemen anzeigen lassen und so Ihre Untersuchungen vereinfachen.

Abb. 16 Bildschirm »User Account Status Changes«

Zeigt fehlgeschlagene Aktionen nach Benutzern gruppiert an, unter anderem Informationen zur Anzahl erfolgloser Leseversuche, Änderungsversuche, Anmeldungen usw.



User Account Status Changes

Shows changes to user accounts status (enabled, disabled, locked, unlocked).

Total Count: 32

Who: ENTERPRISE\DC1$

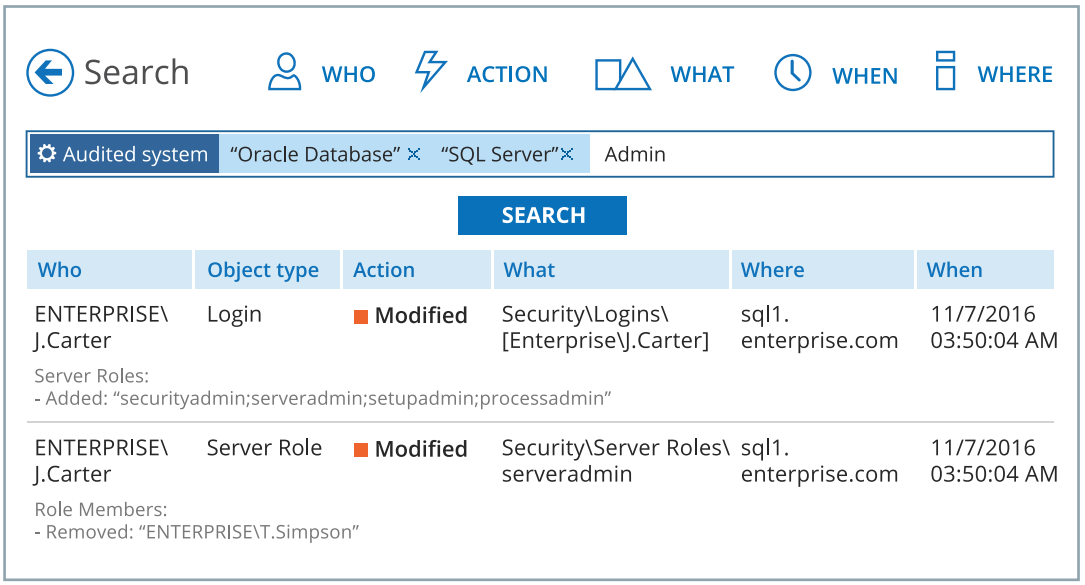
Action	What	When
■ Locked Domain Controller: dc1.enterprise.com Workstation: WIN-46OJH7MQNFT	\Enterprise\Users\Domain Admins	8/22/2016 1:13:26 PM
■ Locked Domain Controller: dc1.enterprise.com Workstation: WIN-74HTEGDHOYE	\com\enterprise\Users\Guest	10/14/2016 3:36:00 PM

Effektivere Untersuchungen durch Analyse von Kontextinformationen

Wenn Sie ein ungewöhnliches oder alarmierendes Ereignis feststellen, das die Sicherheit von Patientenakten gefährden könnte, müssen Sie dieses Problem genauer untersuchen. Durch den Zugriff auf möglichst umfassende Kontextinformationen sind Sie in der Lage, effektiver auf Vorfälle zu reagieren. Netwrix Auditor enthält leistungsstarke Suchfunktionen, mit denen Sie das tatsächliche Ausmaß und den Schweregrad eines Problems schneller und einfacher bestimmen können.

Abb. 17 Bildschirm »Suche«

Wenn Sie ein verdächtiges Ereignis oder eine Kette von Ereignissen feststellen, können Sie mit unserer interaktiven Google-ähnlichen Suchfunktion analysieren, wie es zu diesen Ereignissen kam. So können Sie optimale Gegenmaßnahmen einleiten, um künftig ähnliche Vorfälle zu vermeiden.



Search WHO ACTION WHAT WHEN WHERE

Audited system "Oracle Database" "SQL Server" Admin

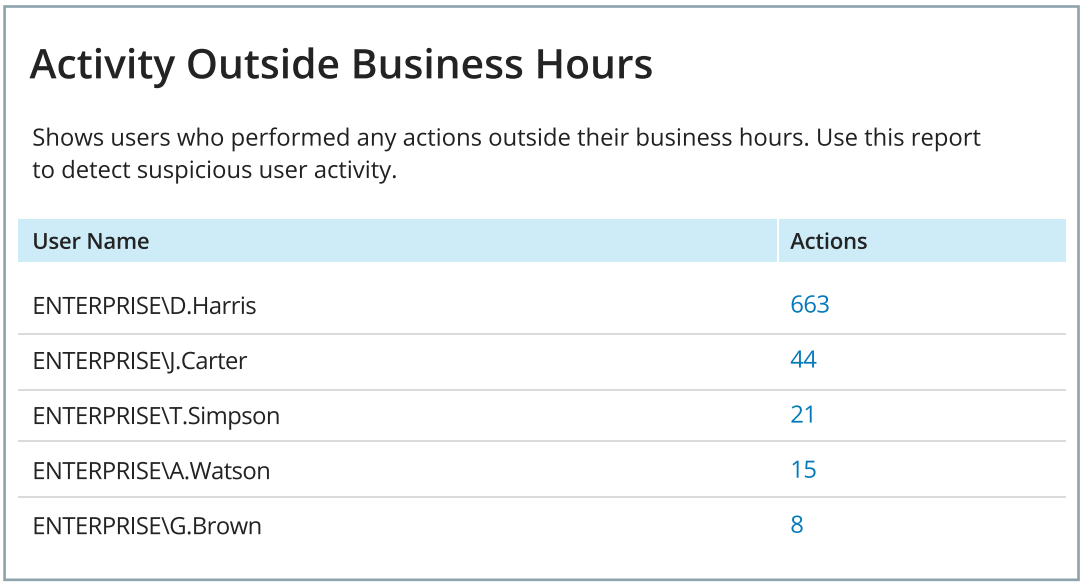
SEARCH

Who	Object type	Action	What	Where	When
ENTERPRISE\J.Carter	Login	■ Modified	Security\Logins\[Enterprise\J.Carter]	sql1.enterprise.com	11/7/2016 03:50:04 AM
Server Roles: - Added: "securityadmin;serveradmin;setupadmin;processadmin"					
ENTERPRISE\J.Carter	Server Role	■ Modified	Security\Server Roles\serveradmin	sql1.enterprise.com	11/7/2016 03:50:04 AM
Role Members: - Removed: "ENTERPRISE\T.Simpson"					

Stärkere Rechenschaftspflicht durch Einblick in die Aktivitäten einzelner Benutzer

Die Gewährleistung der Sicherheit von Patientendaten setzt voraus, dass Ärzte, Auftragnehmer, Geschäftspartner und IT-Mitarbeiter mit weitreichenden Rechten für ihre Aktivitäten zur Rechenschaft gezogen werden können.

Netwrix Auditor stellt Berichte mit Analysen des Benutzerverhaltens und von Blind Spots bereit, beispielsweise zu Aktivitäten außerhalb der Geschäftszeiten (»Activity Outside Business Hours«). Anhand dieser Nachweise können Sie einzelne Personen für Verstöße gegen Richtlinien zur Rechenschaft ziehen.



Activity Outside Business Hours

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

User Name	Actions
ENTERPRISE\D.Harris	663
ENTERPRISE\J.Carter	44
ENTERPRISE\T.Simpson	21
ENTERPRISE\A.Watson	15
ENTERPRISE\G.Brown	8

Abb. 18 Bildschirm »Activity Outside Business Hours«

Zeigt die Benutzer an, die außerhalb der üblichen Geschäftszeiten Aktionen durchgeführt haben. Mithilfe dieses Berichts können Sie verdächtige Benutzeraktivitäten aufdecken.

Anmerkungen

Abb. 16 - 18 | Abbildungsnachweis Netwrix Auditor 9.5

III. Nachweis der Effektivität Ihrer Kontrollen und zuverlässiges Bestehen von Compliance-Audits

Wir sind stets darum bemüht, unsere Prozesse zu verbessern und die Abläufe für unsere Mitarbeiter und Patienten einfach und zugleich sicher zu gestalten. Mit Netwrix Auditor haben wir sowohl unsere gesamte Umgebung als auch die einzelnen Anwendungen im Blick. So können wir unsere Ziele umsetzen und unseren Compliance-Prozess optimieren.

Texas Children's Hospital

Unternehmen und Organisationen, die personenbezogene Daten oder persönliche Gesundheitsinformationen verarbeiten, müssen eine Vielzahl von Gesetzesvorschriften und behördlichen Auflagen einhalten. Das Nichtbestehen eines offiziellen Audits zieht in der Regel hohe Bußgelder und Imageschäden für das Unternehmen nach sich. Eigene interne Bewertungen sind eine sinnvolle Maßnahme, doch ist der Nachweis der Compliance alles andere als einfach. Prüfer geben sich selten damit zufrieden, einfach nur Ihre Richtlinien zu lesen, sondern haben meist klare Erwartungen und Vorgaben, was die praktische Umsetzung dieser Richtlinien betrifft. Mit anderen Worten: Um Audits zu bestehen, müssen Sie die Wirksamkeit Ihrer Sicherheitsmaßnahmen in der Praxis nachweisen können.

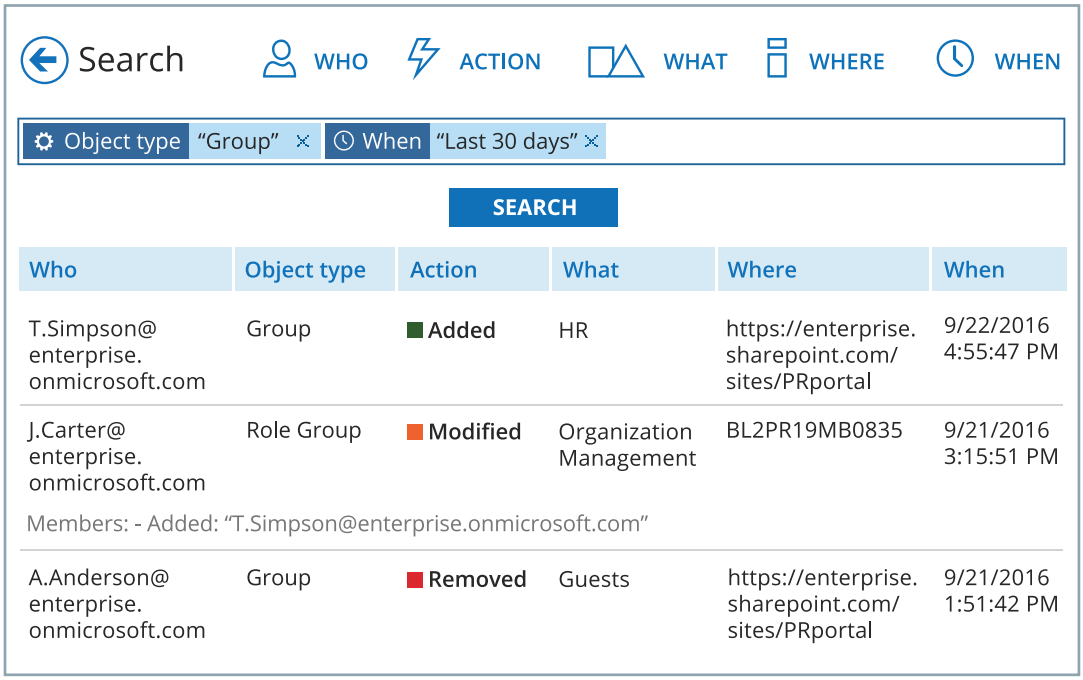
Mit Netwrix Auditor können Unternehmen im Gesundheitswesen viele Anforderungen von Prüfern erfüllen, da sie über die nötigen Überwachungsfunktionen verfügen, um sensible persönliche Gesundheitsinformationen vor Risiken zu schützen. Über die Plattform können sie vordefinierte Compliance-Berichte sowie zahlreiche zusätzliche Compliance-Funktionen nutzen. Damit können die für die Informationssicherheit zuständigen Mitarbeiter ihre Aufgaben sowohl vor als auch während eines Audits effizienter erledigen, sodass das Unternehmen die geforderten Nachweise einfacher und schneller erbringen kann und bessere Audit-Ergebnisse erzielt.

Schnellere Vorbereitung auf interne und externe Bewertungen

Die Vorbereitung auf bevorstehende Audits nimmt in der Regel viel Zeit in Anspruch und bedeutet viel Arbeit. Netwrix Auditor vereinfacht das Abrufen und Aufbereiten von Daten, die von Prüfern sehr wahrscheinlich angefordert werden. Dadurch können Sie den Zeitaufwand für die Vorbereitung verringern. Mithilfe einer interaktiven Suchfunktion können Sie benutzerdefinierte Berichte erstellen, die Antworten auf mögliche Fragen in den Checklisten Ihrer Prüfer liefern. Sie können diese Berichte speichern, damit sie bei einer tatsächlichen Prüfung schnell abrufbar sind.

Abb. 19 Bildschirm »Suche«

Wenn Sie ein verdächtiges Ereignis oder eine Kette von Ereignissen feststellen, können Sie mit unserer interaktiven Google-ähnlichen Suchfunktion analysieren, wie es zu diesen Ereignissen kam. So können Sie optimale Gegenmaßnahmen einleiten, um künftig ähnliche Vorfälle zu vermeiden.



Erfüllen der Erwartungen von Prüfern

Das Erzielen von gesetzlicher Compliance kann viele verschiedene Aspekte umfassen, von der Gewährleistung von physischer Sicherheit der Server, die sensible Daten enthalten, bis zur umgehenden Meldung von Sicherheitsverletzungen. Da diese Anforderungen so vielfältig sind, ist es sehr unwahrscheinlich, dass Sie eine DSGVO-Software oder eine Datenmanagementlösung finden, die alle möglichen Compliance-Anforderungen erfüllt. Wenn Sie sich für eine GDPR-Lösung entscheiden, sollten Sie wissen, welche DSGVO-Anforderungen sie erfüllen kann und wie sie sich mit Ihren Ansprüchen deckt.

Netwrix Auditor bietet unternehmensweite Transparenz über lokale und cloudbasierte Systeme und Anwendungen hinweg, damit Sie ordnungsgemäße Informationssicherheitskontrollen aufbauen und prüfen können, dass diese Kontrollen mit den spezifischen Anforderungen der DSGVO-Datenschutzvorgabe im Einklang sind:

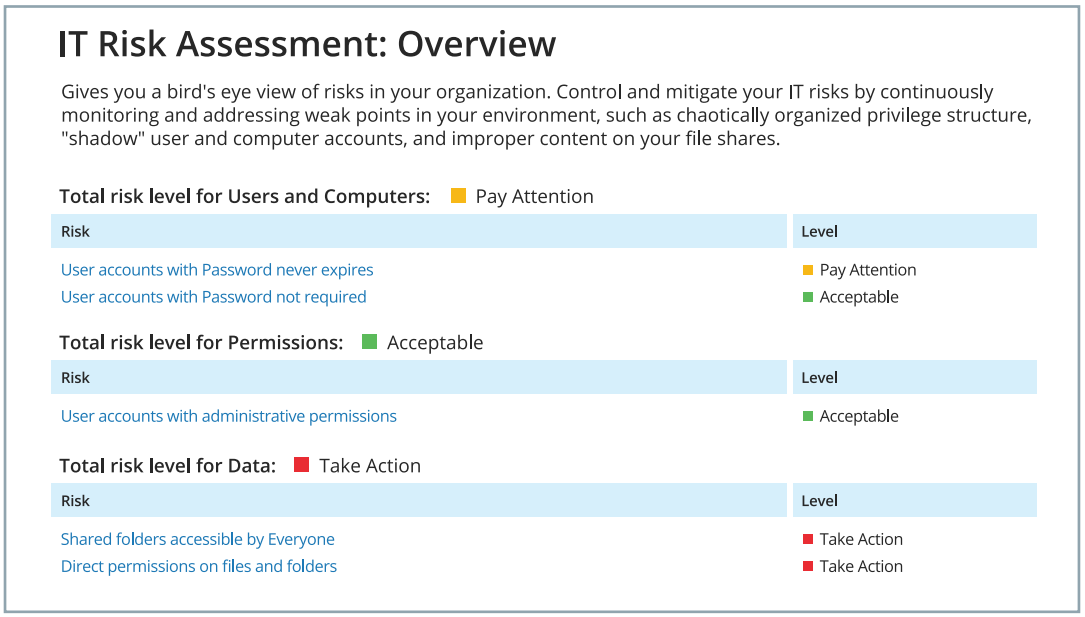
Kapitel II. Grundsätze	Artikel 5. Die Grundsätze beziehen sich auf die Verarbeitung persönlicher Daten: §1(f); §2
Kapitel III. Rechte des Datensubjekts	Artikel 15. Zugriffsrecht durch das Datensubjekt: §1 (b) Artikel 16. Nachbesserungsrecht Artikel 17. Recht auf Löschung (»Recht auf Vergessenwerden«): §1 Artikel 20. Recht auf Datenübertragbarkeit: §1
Kpitel IV. Controller und Verarbeiter	Artikel 24. Verantwortlichkeit des Controllers: §1 Artikel 25. Datenschutz nach Design und nach Standard: §1; §2 Artikel 32. Sichere Verarbeitung: §1 (b, c, d); §2; §4 Artikel 33. Benachrichtigung der Aufsichtsbehörde über eine Verletzung personenbezogener Daten: §1; §3 (a) Artikel 34. Kommunikation einer Verletzung personenbezogener Daten an das Datensubjekt: §1

Starten Sie Ihr DSGVO-Compliance-Programm mit einer Bewertung der wichtigen IT-Risiken

Das Gewährleisten von Sicherheit für regulierte Daten reicht nicht aus, wenn Ihre Sicherheit insgesamt niedrig ist und von Cyberkriminellen einfach durchbrochen werden kann. Stellen Sie zunächst sicher, dass Sie über starke Identitäts- und Zugriffseinstellungen verfügen und dass es keine exponierten Daten in Ihrem Netzwerk oder potenziell schädliche Dateien auf IhrenUnternehmensdateiservern gibt.

Abb. 20 Bildschirm »IT Risk Assessment: Overview«

Bietet Ihnen einen umfassenden Überblick über die Risiken in Ihrem Unternehmen. Kontrollieren und dämmen Sie IT-Risiken ein, indem Sie die Schwachstellen in Ihrer Umgebung kontinuierlich überwachen und beheben. Hierzu gehören unübersichtliche Berechtigungsstrukturen, Schattenkonten für Benutzer und Computer sowie ungeeignete Inhalte auf Ihren Dateifreigaben.

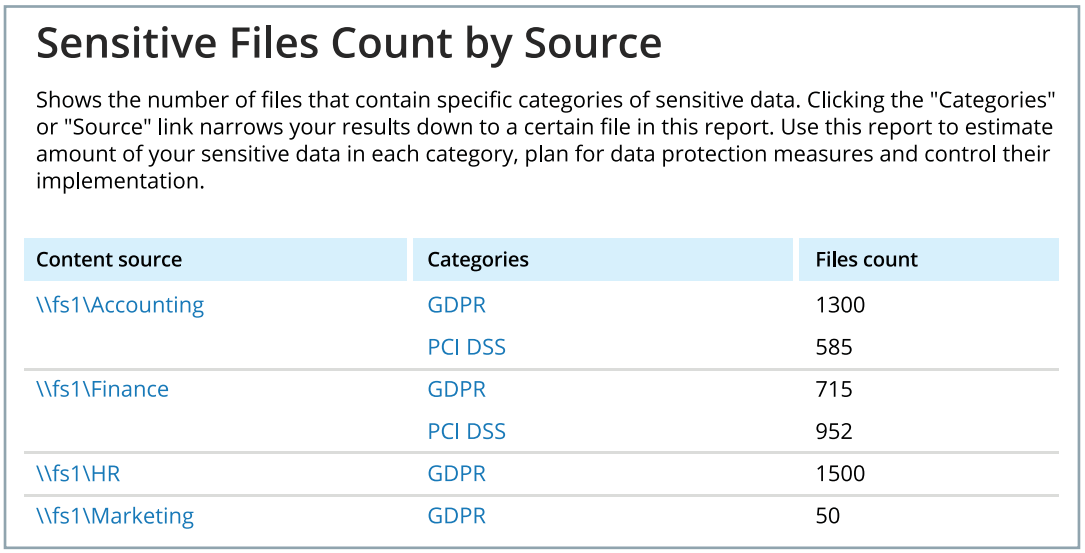


Ermitteln des genauen Speicherorts von DSGVO-Daten

Ermitteln Sie, welche Dateien und Ordner Daten enthalten, die der DSGVO unterliegen. So können Sie eine starke Datenschutzrichtlinie erarbeiten und implementieren und Ihre Data-Governance-Prozesse optimieren. Mit der Datenerkennungstechnologie in Netwrix Auditor können Sie auswählen, welche Kategorien von sensiblen Daten Sie ermitteln möchten.

Abb. 21 Bildschirm »Sensitive Files Count by Source«

Zeigt die Anzahl der Dateien an, die sensible Daten bestimmter Kategorien enthalten. Über die Links »Categories« und »Source« können Sie die Ergebnisse eingrenzen, um die gewünschten Dateien anzuzeigen. Mithilfe dieses Berichts können Sie die ungefähre Menge sensibler Daten in den einzelnen Kategorien ermitteln, Datenschutzvorkehrungen planen und deren Umsetzung steuern.



Optimieren des Datenschutzes mit einer strikten Kontrolle der Zugriffsrechte

Gewährleisten Sie Datensicherheit, indem Sie alle Berechtigungen nach dem Least-Privilege-Prinzip anpassen, damit sensible Ressourcen nur für autorisierte Mitarbeiter zugänglich sind. Ermitteln Sie ganz einfach Benutzer mit übermäßigen Zugriffsrechten, um das Risiko von Datenschutzverletzungen zu minimieren.

Abb. 22 Bildschirm »Sensitive File and Folder Permissions Details«

Zeigt die Zugriffsberechtigungen für Dateien und Ordner an, die sensible Daten bestimmter Kategorien enthalten. Mithilfe dieses Berichts können Sie erkennen, welche Benutzer aufgrund ihrer Gruppenzugehörigkeit oder direkt erteilter Berechtigungen auf eine bestimmte Datei oder einen bestimmten Ordner zugreifen können. Sie können außerdem feststellen, für welche sensiblen Inhalte andere Berechtigungen erteilt wurden als für den übergeordneten Ordner.

Sensitive File and Folder Permissions Details

Shows permissions granted on files and folders that contain certain categories of sensitive data. Use this report to see who has access to a particular file or folder, via either group membership or direct assignment. Reveal sensitive content that has permissions different from the parent folder.

Object: \\fs1\Accounting (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\J.Carter	Full Control	Group
ENTERPRISE\T.Simpson	Full Control	Directly
ENTERPRISE\A.Brown	Full Control	Group

Object: \\fs1\Accounting\Contractors (Permissions: Different from parent)
Categories: GDPR

Account	Permissions	Means granted
ENTERPRISE\M.Smith	Full Control	Group
ENTERPRISE\A.Gold	Full Control	Group

Sicherstellen einer zeitnahen Reaktion auf verdächtige Benutzeraktivitäten rund um die persönlichen Daten von EU-Bürgern

Seien Sie bei anomalen Ereignissen rund um regulierte Daten wachsam, damit Sie diese Daten vor nicht autorisierten Aktivitäten schützen und den Datenschutz gewährleisten können.

Abb. 23 Bildschirm »Warnmeldungen«

Mithilfe von Warnmeldungen können Sie sich umgehend über unerlaubte Aktivitäten benachrichtigen lassen und auf diese Weise Sicherheitsverletzungen verhindern.

Netwrix Auditor Alert

Suspicious access to the Customer Data folder

Who:	ENTERPRISE\J.Carter
Action:	Read
Object type:	Folder
What:	\\fs1\Shared\Finance\EU Customer Data
When:	3/2/2018 5:55:12 PM
Where:	FS1
Workstation:	172.17.2.41
Data source:	File Servers
Monitoring plan:	WFS Monitoring
Details:	Date created: "1/15/20175 5:50:45 PM"

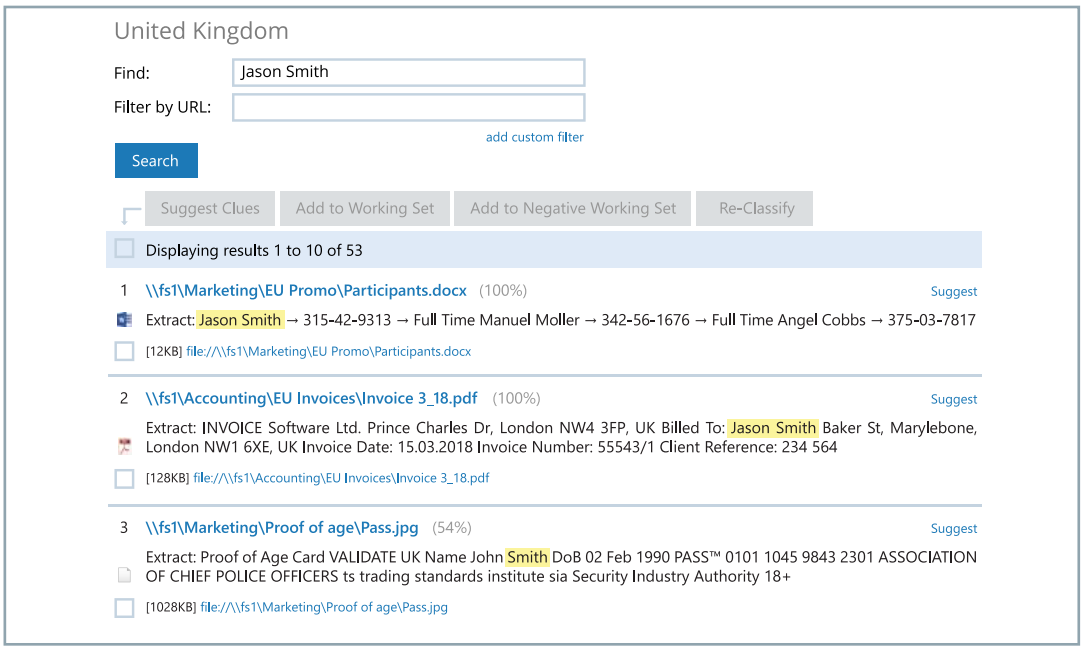
This message was sent by Netwrix Auditor from **audit.enterprise.com.**

Einhalten der Vorgabe »Recht auf Vergessen-werden«

Ermitteln Sie auf Ihren Dateiservern schnell alle Daten zu EU-Bürgern, die ihr Einverständnis zur Verarbeitung ihrer persönlichen Daten zurückgezogen haben, damit Sie sie vollständig löschen können.

Abb. 24 Bildschirm »Suche«

Wenn Sie ein verdächtiges Ereignis oder eine Kette von Ereignissen feststellen, können Sie mit unserer interaktiven Google-ähnlichen Suchfunktion analysieren, wie es zu diesen Ereignissen kam. So können Sie optimale Gegenmaßnahmen einleiten, um künftig ähnliche Vorfälle zu vermeiden.

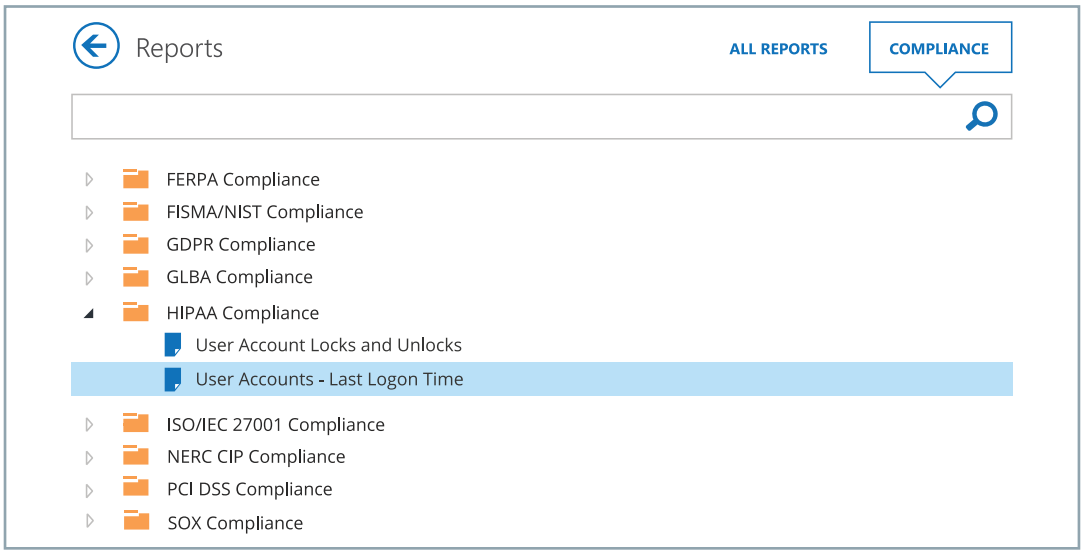


HIPAA-Compliance

Netwrix Auditor stellt vorkonfigurierte Compliance-Berichte bereit, die viele der speziell für das Gesundheitswesen geltenden Compliance-Anforderungen unterstützen. Das Berichtspaket für die HIPAA-Compliance enthält beispielsweise verschiedene Sicherheitsberichte, mit denen Sie nachweisen können, dass Ihre internen Kontrollen in der IT-Umgebung ausreichenden Schutz für die Krankenakten von Patienten und andere persönliche Gesundheitsinformationen bieten.

Abb. 25 Bildschirm »Berichte«

Die Lösung Netwrix Auditor für die Überwachung von IT-Infrastrukturen enthält zahlreiche vordefinierte Berichte, mit denen Sie Compliance- und Management-Anforderungen problemlos einhalten können.



Erbringen Sie den von Prüfern geforderten Nachweis, dass Ihr Informationssicherheits-Team und andere Mitarbeiter regelmäßig automatische Berichte und E-Mail-Benachrichtigungen zur Sicherheit sensibler Daten erhalten.

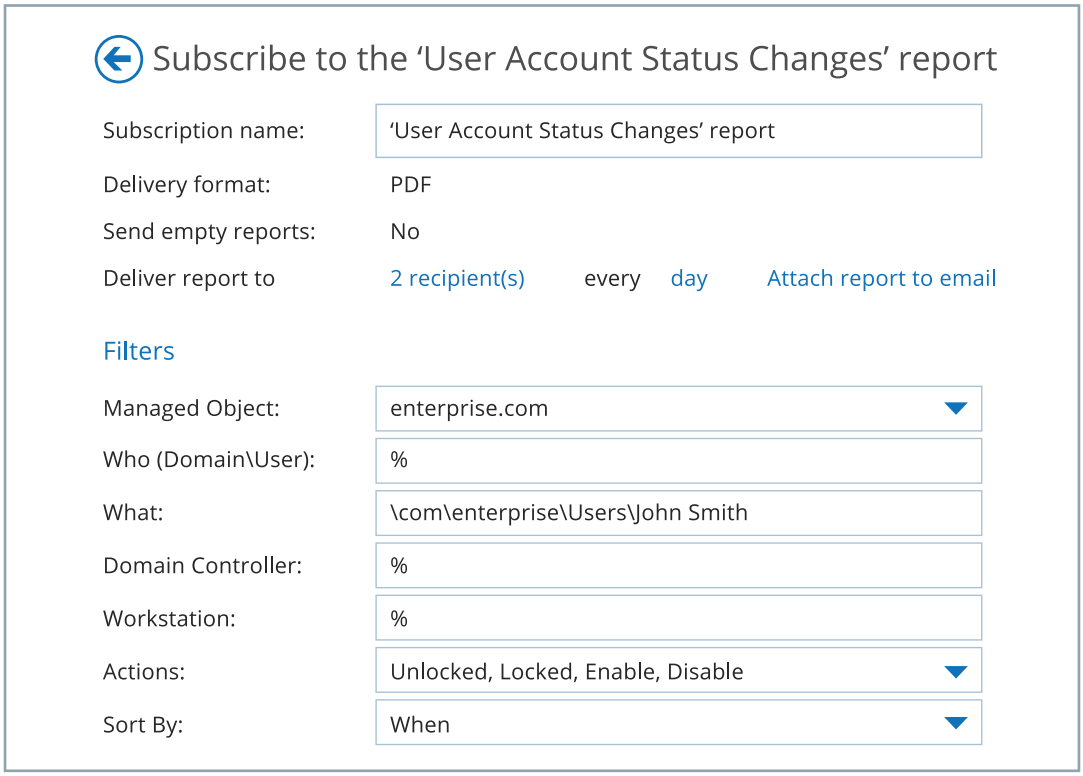


Abb. 26 Bildschirm »Abonnieren des Berichts ›User Account Status Changes‹«

Zu den Änderungen, die ein Hinweis auf böswillige Aktivitäten sein können, zählen die Erstellung zahlreicher neuer AD-Benutzerkonten mit erweiterten Berechtigungen, eine große Zahl inaktiver Benutzerkonten, AD-Benutzerkonten, die deaktiviert oder auf verdächtige Weise geändert wurden, sowie Konten, die nach längerer Inaktivität plötzlich wieder aktiv genutzt werden. Durch die kontinuierliche Überwachung solcher Änderungen können IT-Experten böswillige Aktivitäten rechtzeitig erkennen und dadurch den unbefugten Zugriff auf sensible Daten verhindern.

Mindern der Komplexität und des Aufwands bei der Einführung von Compliance-Prozessen

Wenn Ihr Unternehmen gerade erst mit der Entwicklung eines Sicherheitsprogramms begonnen hat, um den komplexen gesetzlichen Vorgaben gerecht zu werden, schafft Netwrix Auditor eine solide Grundlage für ein solches Programm. Die einsatzbereiten Compliance-Berichte unterstützen Sie bei der Implementierung der notwendigen Kontrollen, während Netwrix leicht verständliche Informationen zu Best Practices für die Einhaltung konkreter Anforderungen bereitstellt.

Anmerkungen

Abb. 19 - 26 | Abbildungsnachweis Netwrix Auditor 9.5

Mapping of Processes and Report Categories to HIPAA Controls*

§ 164.308 Administrative safeguards. (HIPAA Security Rule)

Control	How to Comply?	Processes and Report Categories
§ 164.308 (a)(1)(i) Security management process	In accordance with implemented policies, review activities in information systems to detect and investigate security violations.	Audit Trail All Changes Configuration Management Policy States Configuration States
§ 164.308 (a)(1)(ii)(A) Risk analysis	Utilize audit trail recorded by Netwrix Auditor, while performing assessment of risks to confidentiality, integrity, and availability of PHI.	Access Control All Changes Integrity Monitoring System Integrity Data Integrity
§ 164.308 (a)(1)(ii)(B) Risk management	Validate that the implemented security measures are sufficient and appropriate relying on organization defined procedures and audit trail produced by Netwrix Auditor.	Data Governance Data Integrity User Activity Configuration Management Configuration Changes Configuration States
§ 164.308 (a)(1)(ii)(C) Sanction policy	To support this requirement please refer to the user activities trail for violations of security policies.	Access Control User Activity Account Management Account States
§ 164.308 (a)(1)(ii)(D) Information system activity review	Utilize built-in capabilities for alerts and on-demand reports to regularly audit activities in organization-defined information systems.	Audit Trail All Changes User Activity

* Abbildung der Prozesse und Berichtskategorien auf die HIPAA-Kontrollen

Im Gegensatz zu vielen anderen Softwarelösungen für das HIPAA-Auditing stellt Netwrix Auditor sofort einsatzbereite Compliance-Berichte bereit, die auf bestimmte HIPAA-Anforderungen und eine Vielzahl anderer einschlägiger Vorschriften ausgerichtet sind. So können Sie Kosten- und Zeitaufwand für Ihre Compliance-Prozesse deutlich verringern.

Fazit

Im Gesundheitswesen ist es heute wichtiger, aber auch schwieriger denn je, die Sicherheit der Daten Ihres Unternehmens und Ihrer Patienten zu gewährleisten. Es gilt, sich vor immer häufigeren und ausgefeilteren Cyberangriffen zu schützen, und Sie müssen regelmäßig die lückenlose Einhaltung einer Vielzahl komplexer Vorschriften nachweisen. Deshalb ist es an der Zeit, in Lösungen zu investieren, die Sie bei diesen Aufgaben unterstützen und dabei Ihren Zeitaufwand verringern.

Weltweit setzen bereits viele namhafte Unternehmen aus dem Gesundheitswesen auf Netwrix Auditor, um die Risiken für ihre sensiblen Daten einzudämmen und gesetzlich vorgeschriebene Audits erfolgreich zu bestehen. Mit Netwrix Auditor können Sie Prüfdaten aus allen wichtigen Systemen Ihrer IT-Organisation – ob in der lokalen Umgebung oder in der Cloud – mühelos erfassen und konsolidieren. Das Sichten unzähliger Protokolle und die aufwendige Suche nach unvollständigen, auf unterschiedliche Systeme verteilten Daten gehört damit der Vergangenheit an: Netwrix Auditor stellt aussagekräftige Informationen in übersichtlichen Dashboards und ausführlichen Berichten bereit, sodass Sie Schwachstellen in Ihrer Umgebung und akute Bedrohungen einfach erkennen und schnell geeignete Gegenmaßnahmen ergreifen können. Leistungsstarke, interaktive Suchfunktionen ermöglichen Ihnen einfachere Untersuchungen. Darüber hinaus können Sie sich mit Netwrix Auditor schneller und mit deutlich weniger Aufwand auf gesetzliche vorgeschriebene Compliance-Audits vorbereiten und diese mühelos bestehen.

Unter www.netwrix.de finden Sie ausführliche Informationen, unter anderem auch dazu, wie Sie Netwrix Auditor in nur 15 Minuten in Ihrer Umgebung implementieren.

Informationen zu Netwrix

Netwrix Corporation hat als erster Anbieter eine Plattform für Transparenz und Governance in lokalen, hybriden und cloudbasierten IT-Umgebungen auf den Markt gebracht. Mehr als 160.000 IT-Abteilungen auf der ganzen Welt setzen auf die Lösungen von Netwrix, um Insider-Bedrohungen in lokalen und Cloud-Infrastrukturen zu erkennen, Compliance-Audits ohne hohen Kostenaufwand zu bestehen und die Produktivität ihrer für IT-Sicherheit und IT-Betrieb zuständigen Teams zu steigern. Netwrix wurde 2006 gegründet. Das Unternehmen hat bereits über 100 Auszeichnungen erhalten und ist sowohl im Ranking »Inc. 5000« als auch in der Liste »Deloitte Technology Fast 500« der am schnellsten wachsenden Unternehmen in den USA vertreten.

Netwrix Auditor ist eine Plattform für Transparenz und Governance, mit der Unternehmen Änderungen, Konfigurationen und Zugriffsrechte in Hybrid-Cloud-Umgebungen kontrollieren und Daten unabhängig vom Speicherort schützen können. Sicherheitsanalysen ermöglichen die Erkennung von ungewöhnlichem Benutzerverhalten und die Untersuchung von Bedrohungsmustern, noch bevor es zu Datenschutzverletzungen kommt.

Netwrix Auditor beinhaltet Anwendungen für Active Directory, Azure AD, Exchange, Office 365, Windows-Dateiserver, Dell EMC-Speichergeräte, NetApp Filer-Appliances, SharePoint, Oracle Database, SQL Server, VMware und Windows Server. Auf der Grundlage einer RESTful API und der Videoaufzeichnung von Benutzeraktivitäten bietet die Plattform einheitliche Transparenz und Kontrolle für sämtliche lokalen und cloudbasierten IT-Systeme.

Weitere Informationen finden Sie unter www.netwrix.de.

Einige unserer Kunden

21st Century Oncology

ACCRETIVE HEALTH

JACKSON HOSPITAL

MOLINA HEALTHCARE

WE MAKE LIVES BETTER
UT HEALTH SCIENCE CENTER
SAN ANTONIO

Texas Children's Hospital

SPEARE Memorial Hospital
A Critical Access Hospital

THE GENEVA FOUNDATION
The future of military medicine. Today

Nützliche Links

Probieren Sie Netwrix Auditor aus

Lokale Bereitstellung

Laden Sie eine kostenlose 20-Tage-Testversion herunter

netwrix.com/go/freetrial

Virtuelle Appliance

Laden Sie unser VM-Image herunter

netwrix.com/go/appliance

Bereitstellung in der Cloud

Implementieren Sie Netwrix Auditor in der Cloud

netwrix.com/go/cloud

Kontaktieren Sie Uns

netwrix.com/social

Twitter

twitter.com/netwrix

Facebook

facebook.com/Netwrix

LinkedIn

linkedin.com/company/455932

YouTube

youtube.com/user/NetWrix

Spiceworks

community.spiceworks.com/pages/NetWrix

Instagram

instagram.com/netwrix/

Impressum

Frank Stratmann*

Website
betablogr.de

Büroadresse
Rubensweg 5, D-9872
Meschede

E-mail
frank@betablogr.de

Netwrix Corporation**

Website
netwrix.de

Firmenzentrale
300 Spectrum Center
Drive, Suite 200, Irvine, CA
92618, USA

Telefonnummer
DE: +49 711 899 89 187
CH: +41 43 508 34 72
AU: +43 72 077 58 72

* Im Auftrag von Netwrix Corporation.