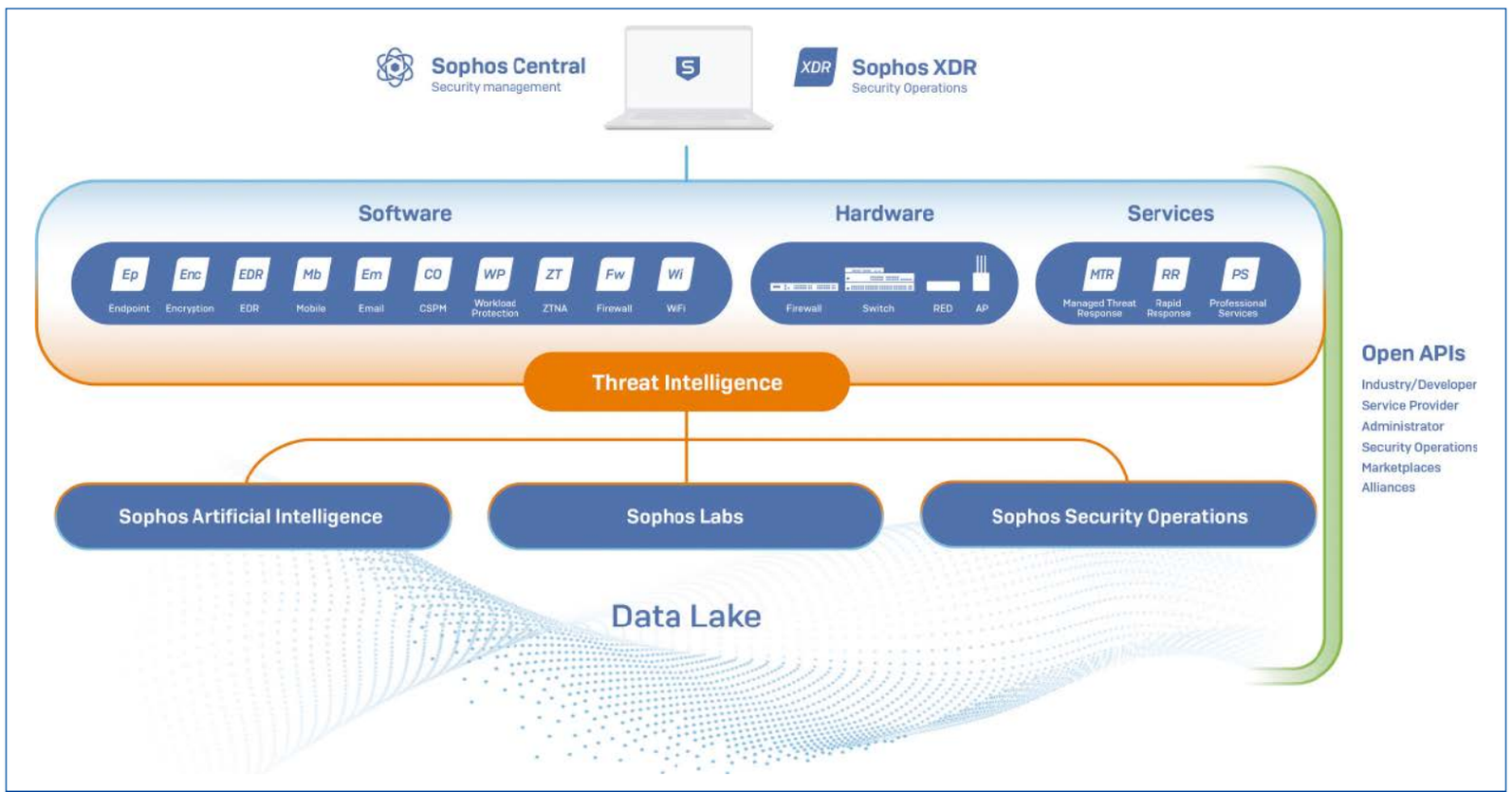
Dreifachschutz für Healthcare-Daten

Nicht nur der Gesetzgeber, auch die aktuelle Gefahrenlage drängt zum Handeln.



Das adaptive Cybersecurity Ökosystem ACE von Sophos lässt alle Elemente in einem IT-Security-Konzept miteinander kommunizieren. Foto: Sophos

Für eine gesetzeskonforme und zeitgemäße IT-Sicherheit in Healthcare-Organisationen sind drei Aspekte entscheidend: optimierte Prozesse, hochkarätige IT-Sicherheitslösungen sowie ein Teamplay aus Technologie und menschlicher Expertise.

Digitalisierung und Transparenz im Sinne der Patienten: schnelle, unkomplizierte Einsicht in Patientendaten und Krankheitsverläufe, Verfügbarkeit von Befunden und digitalen Bildern, kein unnötiger Zeitverlust durch stets neue Anamnesen etc. – das u. a. ist es, was mit dem Patientendatenschutzgesetz (PDSG) und der elektronischen Patientenakte (ePA) angestrebt wird. Seit 2021 können Patienten demnach die Speicherung von medizinischen Befunden, Arztberichten etc. verlangen. Mit dem Jahr 2022 wurde diese Option erweitert, z. B. um den Impfausweis oder den Mutterpass. Neben inhaltlichen Bedingungen beschreibt das Gesetz auch Vorgaben für die Sicherheit von Patientendaten. Es sind hohe Standards gefordert. So besteht seit dem 1. Januar 2022 auch für Krankenhäuser die Verpflichtung, die Vertraulichkeit, Integrität und Verfügbarkeit der sensiblen Informationen sowie die Sicherheit der IT und ihrer Prozesse zu gewährleisten. Was hier vom Gesetzgeber vorgeschrieben wird, erweist sich auch vor anderem Hintergrund als das Gebot der Stunde: Zunehmend zielen Cyberangriffe auf das Gesundheitswesen, denn die höchst sensiblen Daten aus diesem Bereich versprechen den Cyberkriminellen äußerst lukrative Darknet-Gewinne. Immerhin bestätigt die Studie von Sophos „State of Ransomware 2021", dass 34 % der Healthcare-Organisationen von Ransomware-Angriffen betroffen sind und 41 % sind sich sicher, dass sie künftig betroffen sein werden.

Wie kann eine gute IT-Sicherheitsprophylaxe aussehen?

Neben Sicherheitslösungen, die den besten technischen Standards entsprechen, ist es sicher notwendig, auch sämtliche datenbezogenen Prozesse zu überprüfen und anzupassen sowie Belegschaften für Gefahren und richtige Verhaltensweisen zu sensibilisieren und zu schulen. Hierfür ist eine Bestandsaufnahme hilfreich, die u. a. folgende Aspekte berücksichtigt: Wie sehen die medizinischen Versorgungsprozesse aus und welche IT-Systeme werden dafür verwendet? Wie sind diese Systeme momentan geschützt? Wie sind Verantwortlichkeiten und Zugriffsrechte geregelt? Welche Maßnahmen sind notwendig, um einen ausreichenden gesetzeskonformen Schutz zu gewährleisten?

Zusätzlich ist es sinnvoll, Notfallpläne, Incident-Response-Pläne, zu entwickeln, wie Sophos sie z. B. auf seinem Blog (https://news.sophos.com/de-de/2022/01/20/gut-vorbereitet-fuer-den-cyber-ernstfall-10-punkte-aktionsplan/) beschreibt. Ein weiterer Faktor, der entscheidend sein kann für den Erfolg einer Sicherheitsstrategie, die sowohl den Gesetzesvorgaben als auch den Herausforderungen der aktuellen Cyberbedrohungslandschaft entspricht, ist die Einbindung der Erfahrungen und Expertise menschlicher Fachleute.

System aus Technologie und menschlicher Expertise

Zusammenfassend gilt also, Richtlinien und Prozesse sowie den existierenden Schutz vor Cybergefahren zu prüfen, mit menschlichen Experten zu ergänzen und mit einer Strategie und einem funktionierenden System zu erweitern. Ein Beispiel hierfür ist das Adaptive Cybersecurity Ecosystem. Hier werden eine weitsichtige Sicherheitsstrategie mit einem effizienten Katastrophenmanagement, einer zeitgemäßen und mehrschichtigen Schutztechnologie und einem spezialisierten Team zusammengeführt, das sich mit der Prävention, der Früherkennung und der Schadensbeseitigung auskennt. Von der Notfallplanung über den präventiven Schutz mit Security-Technologie und künstlicher Intelligenz bis hin zu menschengeführter Erkennung und Bekämpfung werden in diesem System alle Maßnahmen zentral koordiniert. Eine besondere Rolle kommt dabei dem Managed Threat Response Service (MTR) zu. Diese hoch kompetenten Teams sind auf das Aufspüren komplexer Bedrohungen und Vorfälle sowie die Bestimmung von Ausmaß und Schwere von Bedrohungen spezialisiert. Sie ergreifen Maßnahmen, um die Bedrohung nicht nur an der auffälligen Stelle, sondern im gesamten Netz der Organisation zu eliminieren, und geben konkrete Ratschläge, um die Ursachen wiederholt auftretender Vorfälle zu bekämpfen.

Im Zusammenwirken all dieser Komponenten aus geplanten Prozessen, modernen IT-Sicherheitslösungen und menschlicher Expertise in einem integrierten Ökosystem besteht ein wirksamer Schutz nicht nur für Patienten und deren Daten. Auch die Gesundheitsorganisationen profitieren in Bezug auf die gesetzlichen Vorschriften, die Compliance und vor allem hinsichtlich der gesicherten Handlungsfähigkeit in einer digitalen Welt, die zunehmend von Gefahren aus dem Cyberraum bedroht wird.

| www.sophos.de |

Was Ärzte über Telefonanlagen wissen sollten

Krankenhäuser und Arztpraxen besitzen oft alte ISDN-Telefonanlagen. Dabei ist die Technik längst durch Internettelefonie (VoIP) ersetzt. Das bietet Vorteile.

Michael Sudahl, Schorndorf

Fast jedes Krankenhaus und jede Arztpraxis hat eine Telefonanlage. Doch längst nicht alle sind auf dem aktuellen Stand. Vor allem in kleineren Häusern sind oft noch alte ISDN-Anlagen installiert. Dabei gibt es diese Übertragungstechnik gar nicht mehr. Sie wurde Ende 2020 ersetzt durch Internettelefonie. „Voice over IP" ist hier der Fachausdruck.

Wer eine neue Telefonanlage beschaffen will, sollte ein paar Fakten kennen. Zuerst wäre zu klären, ob die neue Anlage in der Cloud – der Datenwolke – installiert sein soll oder nicht. Vor allem bei Praxen mit mehreren Ärzten oder bei Krankenhäusern mit verschiedenen Gebäudeteilen oder Standorten empfiehlt sich die Cloud. Denn hier überwiegen die Vorteile gegenüber einer Installation auf dem eigenen Server im Keller.

Idealerweise werden alte Tischtelefone ersetzt durch eine Software, ein Softphone, das auf Notebook oder PC installiert ist. Wer telefonieren will, braucht nur noch diese App und ein Headset. Hinzu kommt ein Preisvorteil von bis zu 20 %, je nach Ausführung und Bedarf des Softphones. Wer sich zudem für einen Provider wie Peoplefone entscheidet, kann mehr als 100 Gespräche gleichzeitig führen – ohne monatliche Grundgebühr. „Was erst mal nach viel klinkt, kann je nach Größe einer Gemeinschaftspraxis oder eines MVZ schnell beansprucht werden", sagt Peoplefone-Geschäftsführer Felix Pflüger.

Stichhaltigster Punkt für das moderne Telefonieren via Cloud dürfte die Flexibilität sein. Denn via Softphone-App lassen sich Prioritäten einrichten. So kann die Software-Anrufe entgegennehmen und an Anrufbeantworter weiterleiten. Das können verschiedene ABs etwa für Rezeptbestellungen, Terminanfragen und Laborbefunde sein. Via Voicemail speichert das System die Anrufe, die sich später en bloc beantworten lassen.

Wichtig ist zu wissen, dass die Technik eine Rund-um-die-Uhr-Betreuung zulässt. Das bedeutet, dass die ABs Tag und Nacht Anrufe entgegennehmen können. Fällt einem Patienten nachts um drei Uhr ein, dass er ein Rezept für ein Asthmaspray braucht, weil sein altes im Moment den letzten Hub gemacht hat, muss er nicht bis zum nächsten Morgen warten, um seinen Rezeptwunsch mitzuteilen. Er kann nachts seinen Arzt anrufen und wird am nächsten Morgen per Mail oder SMS benachrichtigt, wann er sein Rezept abholen kann bzw. wird ihm demnächst direkt sein E-Rezept zugeschickt.

Wer über die Cloud telefoniert, kann Heimarbeitsplätze einrichten. So können Ärzte und MFAs Schreib- oder Abrechnungsarbeiten online von zu Hause aus und via sicherem VPN-Zugang erledigen und sind zugleich unter ihrer Praxisnummer erreichbar. „Teure Rufumleitungen aufs Handy entfallen", erklärt Pflüger.

Ist das Softphone zusätzlich mit der Patienten-Kartei verknüpft, sehen die Kollegen am Empfang, wer anruft. Sie bekommen mit der Annahme des Gesprächs die Patientenakte auf den Bildschirm gespielt und sehen, wer der Anrufer ist, und mit hoher Wahrscheinlichkeit auch, was er möchte. Auch merkt sich eine moderne TK-Anlage die letzten Verbindungen. Sie findet somit bei einem erneuten Anruf den direkten Ansprechpartner. Der zeitfressende Umweg über die Zentrale entfällt.

Interessant ist auch die intuitive Bedienung der Software. Dicke Handbücher sind passé. Stattdessen lässt sich ein Softphone am Bildschirm, mit Maus und per „Drag and Drop" bedienen. Die Einarbeitung in die neue Telefonanlage geht deutlich schneller und effizienter. Selbst Mitarbeiter, die weniger IT-affin sind, gewinnen rasch einen Überblick und können schnell mit dem Programm arbeiten.

Auch interessant ist das Hosting virtueller Anlagen. Das sollte auf jeden Fall auf einem Server stattfinden, der in Deutschland steht und damit der DSGVO unterliegt. Damit ist gewährleistet, dass personenbezogene Daten sicher sind vor Zugriffen von außen. In diesen Kontext fällt auch die Sicherheit nach einem elektronischen Absturz der TK-Anlage, sodass diese binnen Minuten wieder verfügbar ist. Zentral gespeicherte Back-ups sorgen dafür. Provider wie Peoplefone bieten zudem „Airbags" an, das sind automatische Rufumleitungen auf ein alternatives Ziel, etwa aufs Handy oder Homeoffice.

Zu guter Letzt hilft eine Online-Telefonanlage auch beim Faxen. Statt Papierstau im Gerät, kommen alle Faxe elektronisch im E-Mail-Fach als PDF-Datei an und können von dort an Kollegen oder Krankenkassen weitergeleitet werden. Zu beachten ist beim Telefonieren und Faxen über VoIP, dass der Internetanschluss mindestens 100, besser 250 Mbit/sec. haben sollte. Für MVZ gilt ein Wert von 1.000 Mbit/sec., weil hier noch mehr Datenvolumen entsteht. Arztpraxen die viele Daten wie Röntgenbilder empfangen und senden, sollten sich Gedanken über einen schnellen VDSL- oder Glasfaser-Anschluss machen. ■

Datenschutz messbar machen

Unternehmen, die ihre Personal-Einsatzplanung verbessern, können viel Geld sparen. Dabei müssen Firmen datenschutzrechtliche Vorschriften beachten. Diese werden oft als lästiges Übel angesehen.

Wie können Firmen Datenschutz umsetzen und sogar davon profitieren? Diese Fragen beantwortet das Projekt EduMiDa – Erfolgreich durch Mitarbeiterdatenschutz, das jetzt gestartet ist: Forscher des Fraunhofer-Instituts für Sichere Informationstechnologie sowie der Universitäten Bremen und Münster untersuchen, wie sich Datenschutz und wirtschaftliche Interessen ergänzen können.

Viele Firmen, etwa Lieferdienste, Logistik-Dienstleister, Supermarktketten, wollen teure Leerlaufzeiten ihres Personals vermeiden und sammeln deshalb persönliche Daten ihrer Mitarbeitenden, etwa über eine Standortbestimmung in Echtzeit. Die Nutzung persönlicher Daten muss allerdings strengen rechtlichen Anforderungen genügen – Verstöße gegen die Datenschutzgrundverordnung (DSGVO) können mit Geldbußen in Millionenhöhe belegt werden und sorgen darüber hinaus für negative Schlagzeilen, wenn einzelne Unternehmen die Privatsphäre ihrer Mitarbeitenden verletzen. Meist sehen Firmen den Arbeitnehmerdatenschutz deshalb als notwendiges Übel.

Ideelle und wirtschaftliche Werte

Hier setzt das Projekt EduMiDa an: Es will zeigen, dass Datenschutz eine Errungenschaft ist, die sowohl Arbeitnehmenden als auch Unternehmen zugutekommt und so zu einem Wettbewerbsvorteil werden kann. „Die DSGVO verlangt, dass Arbeitgeber technische und organisatorische Maßnahmen zum Schutz von Daten angemessen umsetzen müssen", erklärt Dr. Annika Selzer, Leiterin des Projekts am Fraunhofer-Institut für Sichere Informationstechnologie. „In EduMiDa schauen wir, wie sich die schwierige Abwägung zwischen Implementierungskosten von Schutzmaßnahmen und den Rechten und Freiheiten der Mitarbeitenden in der Praxis umsetzen lässt."

Datenschutz messbar machen

Unternehmen, die sensible Daten von Mitarbeitenden für bessere Betriebsabläufe erheben müssen, profitieren davon, wenn sie übersichtlich ausweisen können, dass sie datenschutzkonform und transparent arbeiten, so die Arbeitsthese der Forschenden in EduMiDa. „Wir glauben, dass Transparenz bei der Datenerhebung hilft, Vertrauen zu fördern, die Zufriedenheit der Arbeitnehmenden zu erhöhen und allgemein für einen guten Ruf des Unternehmens zu sorgen", sagt Annika Selzer.

Um dies zu erreichen, entwickeln die Forschenden in EduMiDa Datenschutzmetriken, die sich aus rechtlichen Anforderungen und technischen Voraussetzungen ergeben. Mit diesen Datenschutzmetriken können Personalplanungssysteme automatisiert geprüft werden, sodass Aufsichtsbehörden, Betriebsräte, aber auch die Mitarbeitenden selbst schnell und übersichtlich sehen können, ob ein System den datenschutzrechtlichen Anforderungen genügt.

Testfall Logistik

Eine Auswahl dieser Metriken wird in einem Demonstrator implementiert und in verschiedenen Anwendungsszenarien aus der Logistik getestet. Ein Beispiel ist der kurzfristige Ausfall einer technischen Anlage auf einem sehr großen Betriebsgelände, nach dem der Einsatz des Personals für die Dauer der Reparatur sinnvoll umgeplant werden muss. Erweiterte Einsatzdaten von Mitarbeitenden, die u. a. die genauen Standorte der Mitarbeitenden in Echtzeit enthalten, können auch zur Bewältigung von Katastrophenfällen genutzt werden, beispielsweise um schnell einen Überblick zu bekommen, wie viele Personen sich in einer brennenden Lagerhalle befinden, oder Ähnliches.

Die Ergebnisse des Projekts werden für alle Firmen relevant sein, die auf die Verarbeitung von persönlichen Daten ihrer Mitarbeitenden für ihre Geschäftsprozesse angewiesen sind, wie Anbieter im öffentlichen Nahverkehr (wie Verkehrsbetriebe, Carsharing- oder E-Scooter-Anbieter), Logistikunternehmen, Zustellerdienste, Supermarktketten u. v. m.

Zum Projekt

Beteiligt an EduMiDa sind Wirtschaftswissenschaftler der Westfälischen Wilhelms-Universität Münster, Forscher der Universität Bremen (Institut für Informations-, Gesundheits- und Medizinrecht) für die datenschutzrechtliche Analyse sowie das Unternehmen p.l.i. solutions aus Gütersloh, der Technologiepartner des Projektes. Konsortialführer ist das Fraunhofer-Institut für Sichere Informationstechnologie SIT, das sowohl datenschutzrechtliche als auch technische Aufgaben des Projektes übernimmt.

Das Projekt wird vom Bundesministerium für Bildung und Forschung über eine Projektlaufzeit von 30 Monaten (Projektstart: 2021) gefördert.

| www.sit.fraunhofer.de |