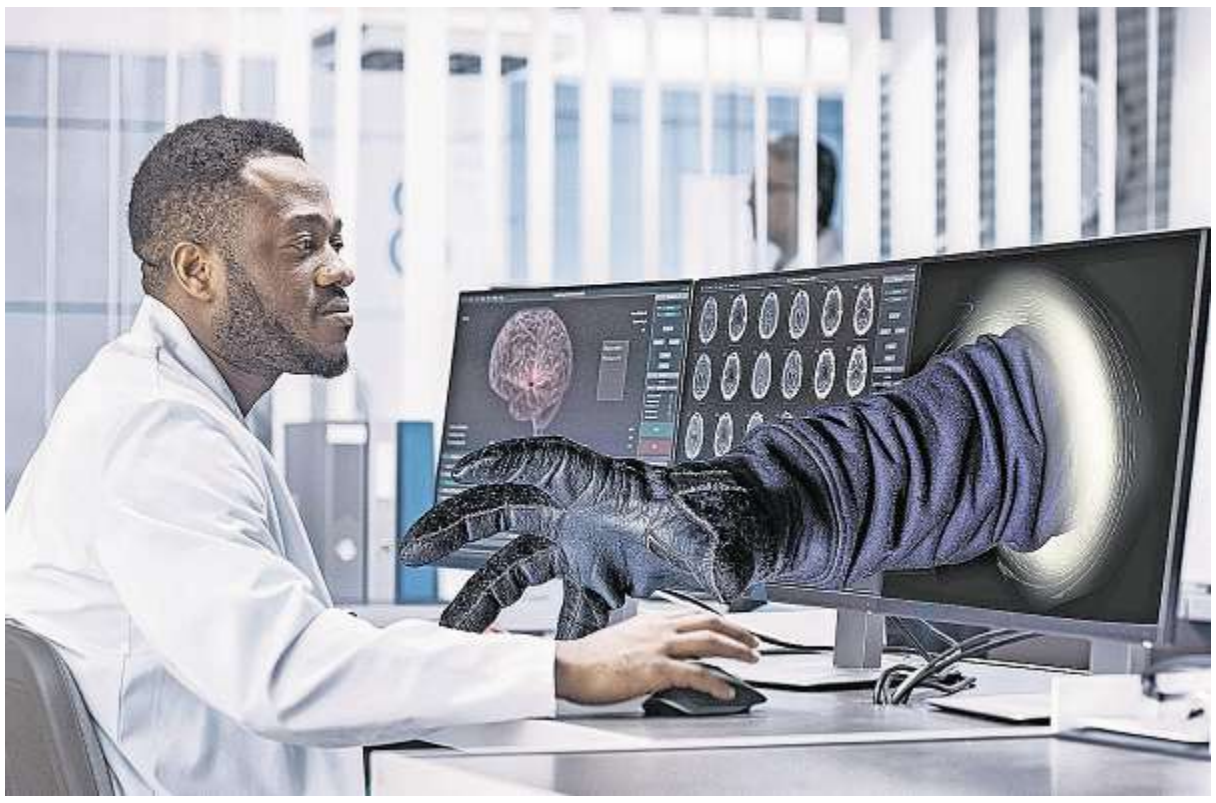
Advertorial

SWS COMPUTERSYSTEME



Hacker erkennen immer mehr den Wert persönlicher Gesundheitsinformationen. Deshalb nehmen Angriffe auf Einrichtungen des Gesundheitswesens zu. Gleichzeitig sorgt die Digitalisierung für immer neue Angriffsflächen.

Foto: Gorodenkoff - stock.adobe.com

Krankenhäuser proaktiv vor Hackern schützen

Krankenhäuser geraten zunehmend ins Visier von Hackern. Die SWS Computersysteme AG rät zu einer proaktiven Sicherheitslösung.

Von Stephanie Burger

REGENSBURG. Reichen die Krankenhauskapazitäten aus, um alle Coronainfizierten optimal behandeln zu können? Diese bange Frage stand am Anfang der Pandemie im Fokus – und war der Ausgangspunkt von Maßnahmen, die verhindern sollten, dass sich viele Menschen gleichzeitig mit dem Coronavirus anstecken.

Doch über die Kapazitätsfrage entscheidet nicht nur die Zahl der Betten, Beatmungsgeräte und des Personals, sondern auch die IT-Struktur, die den Krankenhausbetrieb am Laufen hält. Besondere Kompetenz und langjährige Erfahrung im Bereich Healthcare-IT hat die SWS Computersysteme AG. Das IT-Systemhaus mit Niederlassungen in Regensburg, Hauzenberg und Nürnberg sorgt in vielen Kliniken in Niederbayern und der Oberpfalz für eine effiziente und sichere IT.

Phishing-Attacken vorbeugen

Wie Markus Leitner, SWS-Niederlassungsleiter in Regensburg, betont, muss sich jeder Digitalisierungsschritt im Sicherheitsansatz widerspiegeln. „Digitalisierung kann ohne IT-Sicherheit nicht erfolgreich sein – das gilt für jedes Unternehmen, insbesondere aber für Gesundheitseinrichtungen. „Hier gilt es, mit besonders schützenswerten Daten umzugehen, denn ein Ausfall zentraler Systeme kann das Leben von Patienten gefährden kann“, sagt Leitner. Deshalb ist eine von SWS entworfene Digitalstrategie immer auch eine IT-Security-Strategie. Das sei umso wichtiger, je mehr Krankenhäuser in den Fokus von Cyberkriminellen gerieten, erklärt Martin Kopp, Security Operations Manager (SOC) bei SWS: „Angriffe auf Einrichtungen des Gesundheitssystems nehmen zu. Hacker haben den Wert der dort gespeicherten persönlichen Gesundheitsinformationen erkannt.“ Ziel der Kriminellen sei es meistens, mithilfe von Ransomware-Trojanern Geld zu erpressen. Der IT-Profi schildert, wie ein solcher Angriff sich häufig abspielt: Über Phishing-E-Mails, also gefälschte E-Mails, wird die Ransomware auf dem PC des Nutzers installiert. Diese Schadsoftware verschlüsselt die Daten auf dem Computer des Opfers. Gleichzeitig wird per Bildschirmnachricht Lösegeld gefordert, damit die Dateien wieder entschlüsselt werden. Aber auch andere Erpressungsformen kommen Kopp zufolge vor. Beispielsweise drohten Angreifer auch damit, die Daten ins Internet zu stellen. „Nicht selten kommt es auch zu Mehrfach-Erpressungen“, berichtet Kopp.

Die drohenden Schäden sind immens – eine geeignete Abwehrstrategie ist deshalb unerlässlich. Doch wie können Klinikbetreiber Phishing- und anderen Attacken vorbeugen, um sich und letztendlich ihre Patienten noch besser zu schützen? Kopp erklärt es: „Der erste Schritt besteht immer darin, die Mitarbeiter zu sensibilisieren. Denn am Anfang eines Angriffs steht immer der Mensch.“ Auf technischer Ebene empfiehlt der Experte ein ganzheitliches Security-Paket – ein Baustein davon ist „Cisco Umbrella“. „Damit werden Angriffe aus dem Internet bereits abgefangen, bevor etwas passiert“, sagt Kopp. Der proaktive Ansatz ist die Besonderheit von Cisco Umbrella: Während die meisten Sicherheitslösungen Bedrohungen erst abwehren, wenn sie das Netzwerk erreicht haben, fungiert Cisco Umbrella als „erste Verteidigungslinie“, wie Kopp erläutert. Dazu nutzt die Lösung die Infrastruktur des Internets selbst – nämlich das Domain Name System (DNS), den Internetstandard für die Zugehörigkeit von IP-Adressen. „Cyberkriminelle haben Malware entwickelt, mit der sie DNS-Einträge ändern. Über diese modifizierten DNS-Einträge können sie ‚bösartige‘ Versionen der legitimen IP-Adressen erzeugen“, erklärt Kopp. Genau an dieser Stelle komme nun der Umbrella, also der Schirm, ins Spiel: „Man kann ihn sich als ein riesiges Telefonbuch nachweislich ‚guter‘ Internetadressen vorstellen. Eingehende Verbindungsanfragen werden mit diesem Telefonbuch abgeglichen. Ist der entsprechende Domainname darin nicht enthalten, wird die Anfrage geblockt, das heißt, sie wird erst gar nicht in eine Netzwerkadresse übersetzt.“

Schnell einsatzbereit

Cisco Umbrella funktioniert ortsunabhängig und jenseits herkömmlicher Netzwerk- und Web-Sicherheitslösungen. „Die Implentierung ist denkbar einfach. Im Prinzip ist Cisco Umbrella in wenigen Minuten einsatzbereit, da keine neue Hardware erforderlich ist. Somit ist das Kosten-Nutzen-Verhältnis optimal“, sagt Kopp. Natürlich müsse diese Lösung in ein umfassendes Sicherheitskonzept mit weiteren technischen sowie organisatorischen Maßnahmen eingebettet werden. „Cisco Umbrella ist ein wichtiger Baustein eines Sicherheitskonzeptes und bietet effektiven Schutz vor DNS-basierten Angriffen.“

Möglicherweise – die genaue Angriffsart wurde bislang nicht kommuniziert – hätte dieser Schirm auch einen Angriff auf ein Krankenhaus im tschechischen Brünn während der Hochphase der Coronakrise abfangen können: Am 12. März war es Hackern gelungen, im Netzwerk des Universitätsklinikums, das eines der größten Covid-19-Testlabore des Landes beherbergt, einen Erpressungstrojaner zu platzieren. Das gesamte Netzwerk musste offline genommen, Operationen verschoben und akute Fälle in andere Krankenhäuser verlagert werden. Es dauerte nach Angaben der Klinik Wochen, bis alle Systeme wieder voll funktionstüchtig waren. Der Fall zeigt einmal mehr: IT-Sicherheit muss oberste Priorität haben, gerade dort, wo es um das Wohl von Patienten geht.

Höchste IT-Sicherheit für Cloud-Services garantiert

SWS hat für ihre Cloud-Services die Zertifizierung nach ISO 27001 erhalten, die für höchste IT-Sicherheitsstandards steht.

Von Stephanie Burger

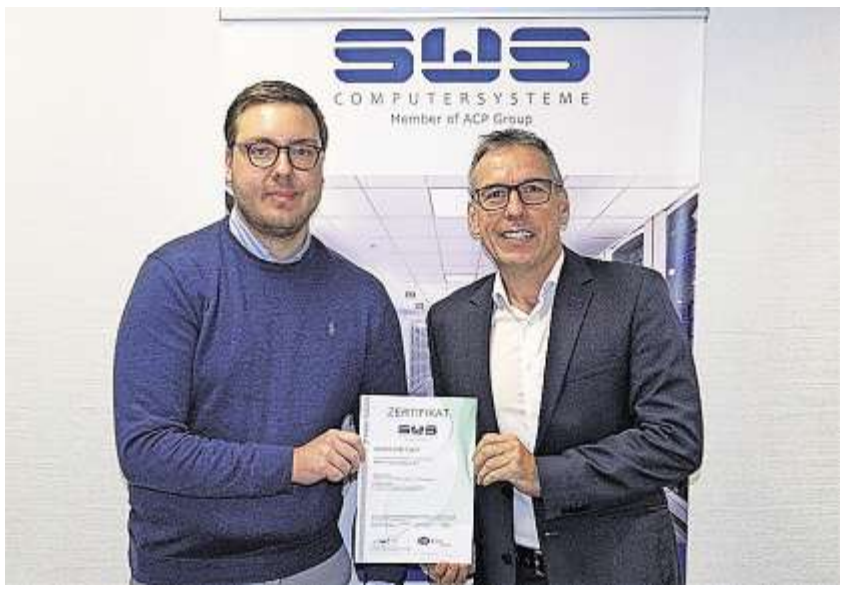
REGENSBURG. Produkte und Dienstleistungen auf höchstmöglichem Informationssicherheitsniveau zu bieten: Das ist der Anspruch der SWS Computersysteme AG. Um diesen zu untermauern, hat das auf die Belange mittelständischer Unternehmen spezialisierte IT-Systemhaus den Weg zur Zertifizierung nach der Norm ISO 27001 beschritten – und ihn nun für den Bereich „Bereitstellung und Betrieb von cloudbasierten IT- und Security-Lösungen“ erfolgreich abgeschlossen. „Die Zertifizierung bescheinigt uns höchsten IT-Sicherheitsstandard. Damit haben wir einen ganz besonderen Meilenstein in der Geschichte unseres Unternehmens erreicht und einen zusätzlichen Mehrwert für unsere Kunden geschaffen“, freut sich Christian Schreiner, Vorstand und Security-Verantwortlicher von SWS.

Die ISO 27001 ist eine eine internationale Norm für Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen. Grundvoraussetzung für eine Zertifizierung ist die Einführung des Informationssicherheits-Management-Systems, kurz ISMS. Die zertifizierungswillige Organisation muss nachweisen, den Grundwerten der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit zu entsprechen.

„Das weltweit anerkannte Zertifikat ist ein Qualitätsmerkmal, das für funktionierende Prozesse und einen verantwortungsvollen Umgang mit sensiblen Daten und Geschäftsprozessen steht“, sagt Schreiner. Der Zertifizierungsprozess sei allerdings relativ komplex und lasse sich nicht einfach nebenbei erledigen. „Wir haben in den vergangenen Monaten mit Hochdruck daran gearbeitet und unsere ohnehin schon guten und sicheren Prozesse noch einmal optimiert.“ Für ein mittelständisches Systemhaus sei eine ISO 27001-Zertifizierung alles andere als eine Selbstverständlichkeit. „Wir sehen das als Investition in die Zukunft.“

Nachdem für SWS die cloudbasierten und die IT-Security-Lösungen besonders wichtige Geschäftsfelder darstellen, wurden diese auch als Ausgangspunkt der Zertifizierung gewählt. Die hohe Qualität der maßgeschneiderten Cloud-Betriebs- und Sicherheitskonzepte von SWS ist mit der Zertifizierung nun auch offiziell nachgewiesen. „Alle Kunden stehen vor der Herausforderung, Teile ihrer IT in die Cloud auszulagern, denn die Vorteile, beispielsweise in Sachen Flexibilität und Skalierbarkeit, liegen auf der Hand. Allerdings spüren wir bei unseren Kunden auch noch etwas Zurückhaltung. Das ist verständlich, denn Cloud-Dienste zu nutzen, bedeutet, Daten einem Dienstleister zu übergeben. Das setzt natürlich ein hohes Maß an Vertrauen voraus. Mit einem ISO-zertifizierten Dienst können wir nun unsere Kunden unterstützen und darlegen, dieses Vertrauen auch zu verdienen“, erklärt Christoph Kelnberger, der gemeinsam mit Martin Kopp für das Zertifizierungsprojekt bei SWS verantwortlich ist. Als nächstes sollen die „Managed Services“ zertifiziert werden.

Der Digitalverband Bitkom geht davon aus, dass Cloud-Dienste durch die Coronakrise einen Schub erfahren werden: Homeoffice, Verwaltungsmodernisierung, Schultransformation und ein genereller Boost bei der IT-Infrastruktur – überall dort würden Cloud-Lösungen eine zentrale Rolle spielen. „Wir erwarten, dass der Digitalisierungsschub im Zuge der Krisenbewältigung auch die Vorbehalte gegenüber der Cloud zunehmend aufweichen wird“, meint auch Schreiner. „Der Druck steigt, Teile oder sogar die gesamte IT-Systemlandschaft in die Wolke auszulagern.“ Dabei dürften jedoch die Security-Anforderungen nicht auf der Strecke bleiben.



Christoph Kelnberger, verantwortlich für das Qualitätsmanagement, und SWS-Vorstand Christian Schreiner mit dem ISO 27001-Zertifikat (v. li.) Foto: SWS

KONTAKT

SWS Computersysteme AG
Im Gewerbepark D 75
93059 Regensburg
Telefon: +49 (0) 941 / 20605-0
info@sws.de
www.sws.de

SWS COMPUTERSYSTEME
Member of ACP Group