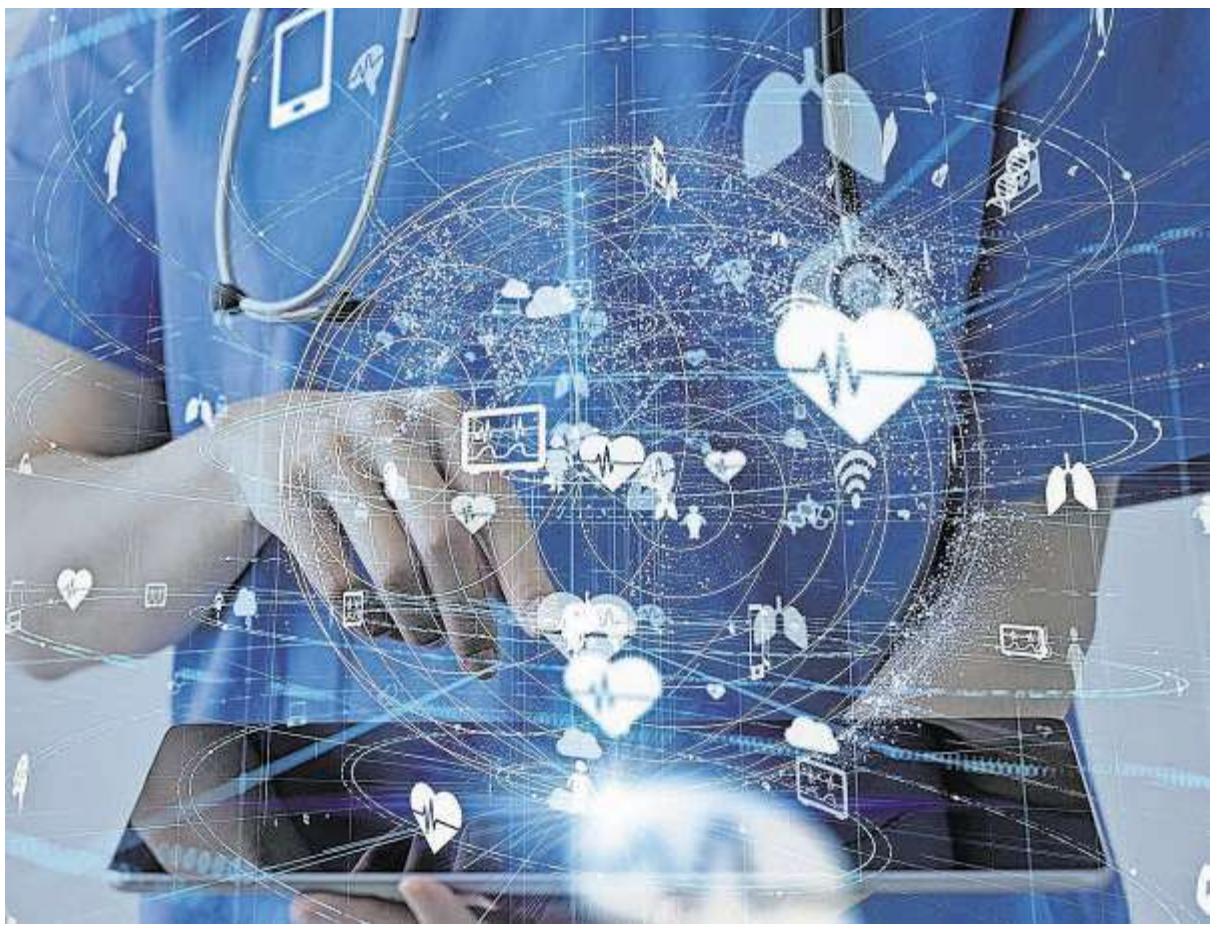
Advertorial

SWS COMPUTERSYSTEME



Ohne IT geht in der Healthcare-Branche heute so gut wie nichts mehr. Dementsprechend hoch müssen die Sicherheitsstandards sein. Foto: metamorworks - stock.adobe.com

„Cybercrime betrifft jeden“

Beim SWS Healthcare Day legte ein Kriminalhauptkommissar die IT-Schwachstellen im Gesundheitswesen schonungslos offen – und die SWS zeigte Lösungen auf.

Von Jonas Raab

LAPPERSDORF. Die Digitalisierung macht auch vor dem Gesundheitswesen nicht Halt. Nur eine ganzheitliche IT-Infrastruktur garantiert reibungslose und wirtschaftliche Abläufe in Krankenhäusern, Arztpraxen oder Pflegeeinrichtungen. Die Menge unterschiedlichster medizinischer Daten wächst von Minute zu Minute. Patientenanamnese und Befunde, biomedizinische Forschungsdaten, Informationen und Daten aus dem medizinischen Alltag:

All diese Daten sind höchst sensibel und besitzen oberste Security-Priorität. Beim ersten Healthcare Day der SWS Computersysteme AG diskutierten Ende September verschiedene Experten digitalisierte Branchenlösungen auf Basis moderner IT-Infrastrukturen. Dabei machten sie eine große Herausforderung im Healthcare-Bereich aus: Cybersecurity. Denn wie gravierend die Folgen sind, wenn Hacker die Gesundheitsbranche ins Visier nehmen, machte insbesondere Kriminalhauptkommissar Peter Vahrenhorst in seinem Vortrag deutlich.

Hackerangriff aus Zufall

Im Cybercrime-Kompetenzzentrum des Landeskriminalamtes Nordrhein-Westfahlen hat es Vahrenhorst täglich mit Security-Vorfällen aller Art zu tun. Am 30. September gab er per Liveschalte ins Aurelium Lappersdorf zahlreichen IT-Leitern, Security-Verantwortlichen, Klinikleitern und -vorständen im hybriden Event spannende Einblicke in die Ermittlungen zum prominentesten Hackerangriff auf eine Gesundheitseinrichtung in Deutschland.

2020 legten Cyberkriminelle aus Zufall – sie hatten es eigentlich auf die benachbarte Universität abgesehen – die Uniklinik Düsseldorf für vier Wochen lahm. Das Krankenhaus musste seine Notfallversorgung vom Netz nehmen, Operationen verschieben und Krankenwagen zu anderen Kliniken umleiten. Dadurch kam es sogar zu einem vermeintlichen Todesfall, weil eine Frau nicht rechtzeitig behandelt werden konnte.

Zwar widersprach Vahrenhorst in seinem Vortrag dem Kausalzusammenhang „Hackerangriff führt zu Todesfall“, den die Bild-Zeitung damals hergestellt hatte, da die Frau laut späteren Ermittlungen wohl auch bei einer umgehenden Behandlung verstorben wäre, aber dennoch warnte der Kriminalhauptkommissar: „Wir waren nicht weit davon entfernt.“ Der Fall mache laut Vahrenhorst vor allem eins deutlich – dass sich niemand in Sicherheit wiegen dürfe. Aussagen à la „Wir sind so klein, uns greift keiner an“ will er deshalb nicht gelten lassen. „Cybercrime betrifft jeden: Privatleute genauso wie Behörden, Wirtschaft und Medizin.“

Vom Anmeldeprozess über den OP, die Radiologie, das Labor bis hin zum einzelnen Lichtschalter im Patientenzimmer, der eine eigene IP-Adresse hat: Nahezu jeder Prozess in einem Krankenhaus ist mittlerweile digitalisiert und muss rund um die Uhr zur Verfügung stehen. „Die fortschreitende Digitalisierung in allen Bereichen bietet Straftätern ganz neue Möglichkeiten“, warnte Kriminalhauptkommissar Vahrenhorst. Das belegen auch die Zahlen: Laut Global Threat Intelligence Report 2021 nahmen IT-Sicherheitsvorfälle im Gesundheitswesen im vergangenen Jahr um 200 Prozent zu. „Die Medizin braucht Spezialisten. Nicht nur in der Chirurgie, auch in der IT“, mahnte Vahrenhorst.

Dass die Uniklinik in Düsseldorf nur aus Versehen Ziel des folgenreichen Angriffs wurde, verdeutlicht die Willkür bei Hackerangriffen. „Cyberkriminelle gehen nicht nach Sympathie, Ethik oder Unternehmensgröße vor. Sie suchen nach Schwachstellen in IT-Systemen und überlegen sich dann, wie sie diese ausbeuten“, erklärte Vahrenhorst. Auch die Healthcare-Branche sei Teil des weltumspannenden Netzes mit Unmengen an Schnittstellen nach außen, die zum Einfallstor für Hackerangriffe werden können. „Ein Netz ist nur so stark wie seine schwächste Stelle“, warnte der Kriminalhauptkommissar.

Ganzheitlicher Ansatz nötig

Der Uniklinik Düsseldorf wurde eine Sicherheitslücke in einer von vielen Unternehmen verwendeten Citrix-Software zum Verhängnis, doch das Sicherheitsproblem in der immer digitaler werdenden Healthcare-Branche liegt tiefer: „Wir gehen nicht ganzheitlich an das Thema Cybersecurity heran, das ist der große Fehler.“ Momentan werde zu sehr in verschiedenen „Silos“ und Einzellösungen gedacht. „Die Medizin ist Teil eines komplexen Systems. Ich stelle immer wieder mit Erstaunen fest, dass Medizin-IT und klassische IT oft nicht miteinander sprechen. Das ist natürlich fatal.“

Welche digitalen Lösungen – immer mit Blick auf die höchstmögliche IT-Sicherheit – es für Healthcare-Einrichtungen aller Art gibt, erklärten die weiteren Referenten des SWS Healthcare Days. Beispielsweise stellte Hans-Martin Kuhn, Senior Security Consultant bei SWS, den rund 90 Teilnehmern des Kongresses verschiedene Verfahren vor, mit deren Hilfe man sich vor Hackerangriffen schützen kann. Sarah Wambach, Cyber Security Business Development bei Cisco, zeigte digitale Möglichkeiten zur Steigerung der Patientensicherheit auf und Oliver Knon, Senior Consultant bei SWS, referierte zu den Themen Netzwerksegmentierung, -transparenz und -security. Die Erkenntnis des Tages: Digitalisierung macht die Healthcare-Branche zukunftsfähig – allerdings nur, wenn die IT-Infrastruktur sicher ist und von Spezialisten betreut und auf dem neusten Stand gehalten wird.

Trends in der IT-Sicherheit: Gewappnet für die Zukunft

Von A wie Awareness bis Z wie Zero Trust: Auf der IT-SA, Europas führender IT-Security-Messe, war der Gesprächsbedarf groß.

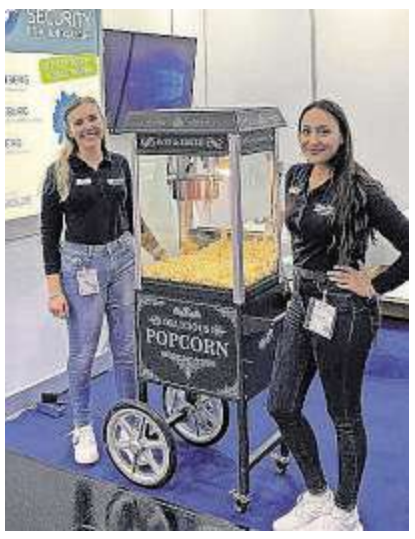
Von Jonas Raab

NÜRNBERG. Dass IT-Sicherheit in allen Branchen rasant an Bedeutung gewinnt, zeigte nicht zuletzt der SWS Healthcare Day am 30. September in Lappersdorf (siehe links). Welche Sicherheitsmechanismen nötig sind, um ein Unternehmen nachhaltig vor Cyberbedrohungen zu schützen, wurde zwei Wochen später in Nürnberg auf der IT-SA, Europas führender Fachmesse für IT-Sicherheit, deutlich. Auch die SWS Computersysteme AG war mit einem großen Messestand und den Security Experten an den drei Messetagen vom 12. bis 14. Oktober vor Ort. Gemeinsam tauschten sie sich mit anderen Security-Experten, Kunden und Partnern über die aktuellen Trends in der IT-Security aus und zeigten Sicherheitsmechanismen gegen Angriffe aus dem Netz auf. Da sich die Arbeitswelt seit der Coronapandemie stark verändert hat und die IT-SA im vergangenen Jahr ausgefallen war, war der Gesprächsbedarf am SWS-Stand groß – auch aufgrund der kürzlich von Bundestag und Bundesrat verabschiedeten Änderungen im Informationssicherheitsgesetz.

Vieles in der IT-Sicherheit drehe sich momentan um Zero-Trust-Lösungen, erklärt SWS Senior Security Consultant Hans-Martin Kuhn. Das zugrunde liegende Vertraue-niemandem-Konzept nimmt Abstand von der Idee eines sicheren Netzwerkbereichs innerhalb eines Unternehmens. Das heißt, jeder Zugriffversuch wird authentifiziert und autorisiert. Man setzt mit Least-Privileged-Access-Lösungen beim Zugriff auf Daten und Informationen an, die direkt und unmittelbar mit dem Geschäftsprozess zusammenhängen. Ein weiterer wichtiger Baustein ist konstantes Monitoring, um Anomalien zu erkennen, die sich in einem Netzwerk abspielen. „IT-Security betrachten wir als ganzheitlich. Man muss sich nicht nur gegen aktuelle Bedrohungen aus dem Internet, sondern auch gegen lokale Angriffsmöglichkeiten schützen“, erklärt Kuhn. Auf der IT-SA 2021 wurde deutlich, dass den Endgeräten in einem Netzwerk deshalb immer mehr Beachtung geschenkt werden muss. Das schaffe man unter anderem mit EDR- und XDR-Produkten, erklärt Kuhn. Endpoint Detection & Response beziehungsweise Extended Detection & Response – dafür stehen die beiden Abkürzungen – erkennen Kompromittierungen auf Endgeräten am Verhalten der Prozesse und bieten Funktionen für die Untersuchung und Eindämmung des Vorfalls. „Weil die Angreifer immer professioneller werden, reichen einfache Virenscanner nicht mehr aus“, sagt Kuhn.

Einen weiteren Trend der IT-Sicherheit und gleichzeitig eine effektive Möglichkeit, sich gegen Cyberkriminelle zu schützen, stellt laut Kuhn ein SASE-Lösungsansatz dar. Der Begriff Secure Access Service Edge mag neu sein, die Idee dahinter allerdings nicht: Der Kern von SASE liegt darin, verschiedene Sicherheitsfunktionen beziehungsweise Gateways in die Cloud zu verschieben. „Wenn man überlegt, wie viele Unternehmensressourcen heute in der Cloud liegen, ist es naheliegend, auch über Sicherheitsfeatures dort nachzudenken“, erklärt Kuhn. Außerdem habe man spätestens in der Pandemie gelernt, wie praktisch es ist, wenn man auch von unterwegs auf Sicherheitsfunktionen zugreifen kann und sich den VPN-Weg ins Unternehmen spart.

Die IT-Sicherheit lebt wie alle Technologiebranchen von der ständigen Weiterentwicklung und Neuerfindung von Trends und Technologien. Deshalb nahmen auf der IT-SA auch neue Themen wie künstliche Intelligenz, Machine Learning, Device-Security und Security-Automatisierung viel Platz ein. „Ob sich diese Trends durchsetzen, wird sich zeigen. Was allerdings sicher ist: In Zukunft spielt der Mix aus verschiedenen Technologien eine größere Rolle, aber auch die Sensibilisierung der Human Firewall im Umgang mit IT-Sicherheit.“



Popcorn und IT-Expertise: SWS Computersysteme auf der IT-SA 2021 Fotos: Tobi Eichenseer

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