CYBERSECURITY: DIGITALE SCHUTZ-AUSRÜSTUNG (NICHT NUR) IN DER PANDEMIE

VMWARE Die Corona-Krise mit ihrer Verlagerung zahlreicher Lebens- und Arbeitsbereiche ins Digitale hat deutlich gemacht, dass Cybersicherheit für Krankenhäuser kein Add-on der Patientenversorgung, sondern geradezu eine Voraussetzung dafür ist. **Carsten Kramschneider**, Manager Solution Engineering, Public, Healthcare & Commercial bei dem Virtualisierungsspezialisten VMware, sieht Krankenhäuser in der Bringschuld und betrachtet das Krankenhauszukunftsgesetz als Chance, bisher Versäumtes nachzuholen.

Die Corona-Krise geht weiter, ob in Wellenform oder als Dauerwelle. Inwieweit ist Corona auch eine Herausforderung für die Krankenhaus-IT?
Die Corona-Krise hat keine neuen Sicherheitsherausforderungen gebracht, aber sie hat diverse Sicherheitsanforderungen noch mal stark in den Vordergrund gerückt, wie ja auch das aktuelle Beispiel der Düsseldorfer Universitätsklinik eindrücklich zeigt. Als die Krise begann, ging es u.a. darum, Mitarbeiter von zu Hause arbeiten zu lassen. Das betraf in Krankenhäusern vor allem die Verwaltung. Da ist schon das eine oder andere Krankenhaus auf uns zugekommen und hat um Hilfe gebeten. Nicht weil die IT-Abteilungen die Thematik „Arbeitsplatz zu Hause“ nicht kennen, sondern einfach weil es sie in dem Umfang, in dem das plötzlich stattfand, dann doch überfordert hat.

Ist IT in Zeiten der Corona-Krise auch eine Art Schutzausrüstung?
Die IT im Krankenhaus – einschließlich des klinischen Arbeitsplatzes – ist meines Erachtens eine Form von Schutzausrüstung: nicht für das Personal, sondern für die Patientendaten. Und dieser Schutz hat natürlich auch viel mit Vertrauen zu tun. Bürger werden einem digitalen Gesundheitswesen nur dann vertrauen, wenn gewährleistet ist, dass die Daten sicher sind.

Wie sehen Ihre konkreten Empfehlungen an die Krankenhäuser aus, mit Blick auf mögliche weitere COVID-19-Wellen, aber auch mit Blick auf andere Krisensituationen?
Das Wichtigste ist, ehrlich zu sein und zu erkennen, ob die eigene Einrichtung für eine Krise gerüstet ist. Da spielen viele Aspekte eine Rolle. Bei VMware haben wir gemeinsam mit Kunden eine Methodik entwickelt, die Krankenhäuser dabei unterstützt, Krisenszenarien zu erkennen und daraus Handlungsbedarfe abzuleiten. Das ist nicht ausschließlich eine Frage von IT, es geht auch um organisatorische und gebäudetechnische Fragen. Wir sprechen von einem Crisis Management Value Wheel: eine geschliffene Methodik, die sehr granular untersucht, in welchen Bereichen mein Unternehmen oder Krankenhaus schon „maximal secure“ ist und wo noch Nachholbedarf besteht.

Ein Spezialthema im Krankenhaus ist die Sicherheit der Medizingeräte, zumal bei COVID-19, wo die Intensivstationen im Fokus stehen. Worauf sollten Krankenhäuser speziell bei diesem Thema achten?
Wir hatten schon vor der Corona-Krise Kunden, die auf uns zukamen und uns gesagt haben, dass sie eigentlich gar nicht so genau wissen, ob einige ihrer zahlreichen Medizingeräte nicht vielleicht mit einem Bein im Internet stehen. Als Spezialist für Security und Infrastrukturen haben wir hier eine Lösung entwickelt, die der Absicherung medizinischer Geräte dient bzw. vor allem auch dem Schutz des Netzwerks vor medizinischen Geräten mit Internetverbindung. Die Lösung besteht darin, dedizierte Netzwerke zu mikrosegmentieren und quasi ein eigenes Netzwerk für die Medizingeräte zur Verfügung zu stellen. Das Kernnetz, das die gesamte IT trägt, ist hermetisch abgeriegelt von Geräten Dritter. Das ist ein Ansatz, der auf sehr viele offene Ohren stößt, nicht nur in Universitätskliniken. Wichtig dabei ist: Wir sind eine „Virtualisierungs-Company“, wir machen das ohne weitere Investitionen in Hardware, physische Netzwerke oder Firewall-Technologien, und zwar so, dass die virtuelle Infrastruktur ihre Agilität nicht verliert. Das lässt sich auch wunderbar skalieren und – zum Beispiel in Klinikverbünden – an unterschiedliche Einrichtungen anpassen. Den Granulierungsgrad der Schutzmaßnahmen bestimmte jeder Kunde selbst.

Sicherheit kostet Geld. Hier will der Gesetzgeber jetzt mit dem Krankenhauszukunftsgesetz nachhelfen, das umfangreiche Fördermittel für Digitalisierung bereitstellt, von denen 15 Prozent in IT-Sicherheit gehen müssen. Wie beurteilen Sie dieses Gesetz?

Carsten Kramschneider
Manager Solution Engineering, Public, Healthcare & Commercial bei VMware

Ich denke, eine gewisse Zweckgebundenheit macht beim Thema IT-Sicherheit Sinn. Mit dem Gesetz zu kritischen Infrastrukturen wurden die Krankenhäuser zu Sicherheitsmaßnahmen verpflichtet, aber ohne eine Antwort zu geben, wie das finanziert werden soll. Möglicherweise werden jetzt gewisse, schon vorher bekannte KRITIS-Investitionen auch vollzogen. Wir können es uns nicht erlauben, dass immer wieder Krankenhäuser vom Netz genommen werden müssen. Wenn sich das nicht ändert, wird die Digitalisierung des Gesundheitswesens nicht vorankommen.

Wie sollten Krankenhäuser mit Blick auf das KHZG vorgehen, und wie kann VMware dabei helfen?

Bei VMware glauben wir nicht, dass die alte Strategie, das Thema Security durch regelmäßige Updates von Virenscanner und Firewall zu adressieren, zielführend ist. Dafür sind die Bedrohungen zu groß geworden. Wir brauchen neue Security-Ansätze, die nicht Dutzende Einzelprodukte nutzen. State-of-the-Art ist eine Sicherheitsarchitektur, und was die Finanzierung betrifft, braucht es eine Herangehensweise, bei der SaaS- und cloudbasierte-Ansätze als Betriebsmittel, und nicht als Einmalinvestitionen gesehen werden. Stichwort KHZG: Krankenhäuser sollten für ihre Sicherheitsarchitektur eigene Security-Projekte aufsetzen, in deren Rahmen die besonderen Schutzbedarfe ermittelt werden. Wir bieten hierzu Beratungsleistungen an und adressieren die identifizierten Defizite dann ganz gezielt. Darüber hinaus unterstützen wir Kunden auch im täglichen Betrieb, etwa indem wir Health Checks durchführen, nach dem Motto: „Wie gesund ist Deine IT-Infrastruktur wirklich?“ Da gibt es oft Aha-Effekte, wenn ein Kunde erkennt, dass ein bestimmter Server mit einem bestimmten Medizingerät kommuniziert, und er das gar nicht auf dem Schirm hatte. Security darf nicht aus Einzelmaßnahmen bestehen, es muss eine Strategie sein. Ein Krankenhaus, das das verstanden hat, ist für weitere Corona-Wellen, aber auch für andere Krisensituationen und Cybercrime-Szenarien, gut gewappnet.

VMWARE GLOBAL, INC.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2, 81829 München
Carsten Kramschneider,
Manager Solution Engineering, Public, Healthcare & Commercial bei VMware
Kontakt: ckramschneider@vmware.com
Tel.: +49-(0)1520-9350638
www.vmware.com/de