KRANKENHÄUSER IN KRITIS-ZEITEN: SECURITY BEGINNT IM RECHENZENTRUM!

VMWARE Berichte über Datenschutzpannen und Cyberangriffe sind an der Tagesordnung. Besonders vulnerabel sind Krankenhäuser. Denn die hantieren mit hochsensiblen Daten, haben gleichzeitig aber oft nicht die nötigen finanziellen Mittel, um sich optimal aufzustellen. **Carsten Kramschneider**, Teamleiter Healthcare & Education bei VMware, Innovationsführer im Bereich Unternehmenssoftware, erläutert, wie Krankenhäuser auf Rechenzentrums- und Infrastrukturebene die Anforderungen an kritische Infrastrukturen erfüllen können.

Wie gefährdet sind Krankenhäuser durch Cyberangriffe? Gibt es dazu aktuelle Daten?
Wir haben in Deutschland inzwischen eine Situation, die schon fast drastisch zu nennen ist. Das gilt in vielen Branchen, aber auch im Gesundheitswesen. Daten einer Roland-Berger-Studie zufolge waren hierzulande 64 Prozent aller Krankenhäuser schon Opfer einer gezielten Cyberattacke oder eines Hackerangriffs. Das ist äußerst brisant, und es zeigt, wie wichtig es war, dass die Gesetzgebung hier im Rahmen des IT-Sicherheitsgesetzes und der Verordnung zur Bestimmung kritischer Infrastrukturen (KRITIS) gegengesteuert hat. Durch den KRITIS-Prozess haben Krankenhäuser eine gute Chance, den digitalen Bedrohungen deutlich besser gerüstet entgegenzutreten.

Formal gelten Krankenhäuser mit mehr als 30 000 stationären Fällen pro Jahr als kritische Infrastrukturen und unterliegen entsprechend den KRITIS-Anforderungen. Wie ist der aktuelle Stand im Gesundheitswesen? Gibt es bereits einen definierten Branchenstandard?
Einen ausformulierten Branchenstandard gibt es bis jetzt noch nicht, was aber nicht heißt, dass es noch keinen Handlungsbedarf gibt. Im KRITIS-Branchenarbeitskreis arbeiten zahlreiche Institutionen der Gesundheitswirtschaft mit Herstellern wie VMware eng zusammen. Und weil VMware einer der Kernprovider von Krankenhausinfrastrukturen ist, kommen auch viele Krankenhäuser auf uns zu, mit denen wir zu KRITIS eng kooperieren. Was die 30 000 stationären Fälle pro Jahr angeht: Ich würde die Frage stellen wollen, ob diese Grenze besonders zielführend ist. 64 Prozent aller Krankenhäuser wurden schon angegriffen – unabhängig von der Größe. Auch kleinere Krankenhäuser sollten sich als kritische Infrastrukturen begreifen und entsprechende Maßnahmen ergreifen.

Was sind die Kernherausforderungen für Krankenhäuser im KRITIS-Prozess?
Rein technisch lautet das wichtigste Stichwort ‚Security'. Krankenhäuser müssen dringend in Security investieren, inklusive neuer Ansätze im Bereich der Netzwerkinfrastruktur. Das Kernproblem ist aber ein anderes: Die Krankenhäuser haben kein Geld. Der Bundesverband der Krankenhaus-IT-Leiterinnen/-Leiter (KH-IT) hat ermittelt, dass den Krankenhäusern in den nächsten fünf Jahren circa 11,6 Milliarden Euro an Investitionsmitteln fehlen. In dieser Situation in großem Maßstab in Security zu investieren, ist kaum möglich. Hier ist auch die Politik gefragt: Sie darf nicht nur Weichen wie KRITIS stellen, sie muss auch die Frage beantworten, wie sich Krankenhäuser nachhaltig finanzieren können. Andere Länder stehen hier besser da, wie beispielsweise die Niederlande. Dort sind die IT-Budgets, gemessen am Umsatz, circa fünf Prozentpunkte höher, entsprechend besser ausgestattet sind die Häuser im Bereich Security.

Wie kann das Unternehmen VMware die Krankenhäuser auf ihrem Weg in Richtung KRITIS-Konformität unterstützen?
Die Lösungen von VMware sind der De-facto-Standard für die Virtualisierung im Rechenzentrum. Entsprechend groß ist unsere Verantwortung, uns im Bereich Security zu engagieren und Kunden dabei zu helfen, die nötigen Maßnahmen umzusetzen. Ein wichtiges Thema ist bei uns die Mikrosegmentierung. Dieses Verfahren sorgt dafür, dass Krankenhäuser unterschiedliche Schutzzonen definieren können. Es gibt die Schutzzone 1, die hermetisch abgeriegelt ist und in der sich kritische Patientendaten befinden. Es gibt aber auch weniger kritische Schutzzonen, etwa jene, in denen sich die Internetnutzung durch Patienten abspielt. Das Entscheidende ist, dass diese Segmentierung auf Software-definierter Ebene stattfindet, und dass nicht versucht wird, unterschiedlich schützenswerte Bereiche durch irgendwelche Hardware-Silos zu trennen. Damit kauft man sich nur neue Probleme ein.

Carsten Kramschneider
Teamleiter Healthcare & Education
bei VMware

Wie relevant sind Infrastrukturservices insgesamt für die KRITIS-Konformität?
Sehr relevant. Das zeigt sich auch daran, dass schon heute viele VMware-Produkte eine Zertifizierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI) durchlaufen. Auch unsere Netzwerk-Security/Mikrosegmentierung befindet sich in der BSI-Evaluierung. Netzwerk und Rechenzentrum sind die Basis der Krankenhaus-IT, und entsprechend muss Security schon auf dieser Ebene ansetzen.

Wie hat man sich ein Mikrosegmentierungsprojekt im Krankenhaus konkret vorzustellen?
Wir bilden ein Team mit relevanten Stakeholdern, also mit Vertretern der IT-Abteilung, aber auch mit dem CEO oder dem Chief Information Security Officer, und versuchen gemeinsam, eine Lösung zu kreieren, die dem individuellen Krankenhaus gerecht wird. VMware kann bei der Umsetzung helfen, aber gleichzeitig ist der Kunde gefordert, denn er muss die relevanten Informationen liefern. Als VMware sind wir da insofern sehr gut aufgestellt, als wir in unserem ‚Team Gesundheit' eine Reihe ehemaliger IT-Leiter aus Krankenhäusern haben, die mit den Kunden auf einem Level kommunizieren können. Was den Zeitaufwand angeht, reden wir von einem mehrmonatigen Projekt. Die dünne Personaldecke vieler Krankenhäuser ist da oft nicht so hilfreich.

Inwieweit decken sich KRITIS-Anforderungen mit jenen, die die DSGVO stellt?
Die Anforderungen überschneiden sich teilweise, aber vor allem ergänzen sie sich. Sowohl aus Datenschutz- als auch aus Datensicherheitsperspektive ist es wichtig, dass nachvollziehbar ist, welcher Mitarbeiter welche Patientendaten im positiven Sinne manipuliert hat. Das ist eine Anforderung der DSGVO, kann aber genauso im Rahmen von KRITIS-Überprüfungen abgefragt werden. Diese Nachvollziehbarkeit ist eine grundsätzliche Anforderung. Sie gilt unabhängig von der Schutzklasse der Daten.

VMWARE GLOBAL, INC.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2, 81829 München
Carsten Kramschneider,
Teamleiter Healthcare & Education
Kontakt: ckramschneider@vmware.com
Tel.: +49-(0)1520-9350638
www.vmware.com/de