arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Organisationen aus dem Gesundheitswesen brauchen bessere Strategien zur Datenwiederherstellung

Von René Claus, EMEA MSP Sales Director bei Arcserve

Organisationen des Gesundheitswesens sind zunehmend durch Ransomware-Angriffe bedroht. Dieses Segment ist für Cyberkriminelle besonders interessant, da die Organisationen aus dieser Branche große Mengen an sensiblen Patientendaten – einschließlich persönlicher Informationen, medizinischer Aufzeichnungen und finanzieller Details – verwalten. Die Aussichten auf hohe Lösegeldsummen sind für die Cyberkriminellen gut. Denn aufgrund der strengen gesetzlichen Sorgfaltspflicht für die Daten und der elementaren Fürsorge für Patienten sind die Organisationen in besonderem Maße daran interessiert, die wichtigen oder vielleicht sogar lebensrettenden Informationen wieder zu bekommen.

Aus diesen Gründen ist die Zahl der Ransomware-Angriffe auf Gesundheitsorganisationen in den vergangenen Jahren stark gestiegen. Laut eines aktuellen Berichts des IT-Security-Unternehmens Sophos geben mehr als zwei Drittel der Gesundheitsorganisationen an, dass sie bereits einen Ransomware-Angriff erlebt haben. Diese Angriffe können wichtige Gesundheitsdienste schnell zum Erliegen bringen. Wenn Patientendaten und medizinische Aufzeichnungen aufgrund kompromittierter Systeme unzugänglich sind, haben nicht nur Ärzte, sondern nahezu alle Mitarbeiter im Gesundheitssektor Schwierigkeiten, eine rechtzeitige und genaue Versorgung zu gewährleisten. Behandlungsverzögerungen, unvollständige Diagnosen und Medikationsinformationen können die Patientensicherheit erheblich beeinträchtigen.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Für viele scheint es der schnellste Weg aus einem Ransomware-Angriff zu sein, die Angreifer zu bezahlen – und darauf zu hoffen, dass die Angreifer die Entschlüsselungs-Codes zur Verfügung stellen, die dann auch funktionieren. Eine Studie von Arcserve zeigt, dass 67 Prozent der Gesundheitseinrichtungen nach einem Ransomware-Angriff Lösegeld gezahlt haben – mehr als in jeder anderen Branche. Es scheint verständlich, dass viele Organisationen das Lösegeld zugunsten der Wiederherstellung der operativen IT-Systeme und zugunsten der Patientenversorgung bezahlen, anstatt das Wohlergehen ihrer Patienten zu riskieren. Wenn ein Krankenhaus angegriffen wird, geht es immerhin nicht nur um die ethischen Aspekte der Bezahlung von Cyberkriminellen, sondern um das Leben der Patienten.

Die vielen Risikofaktoren für Ransomware im Gesundheitswesen

Ein weiterer Grund, weshalb Organisationen der Gesundheitsbranche Lösegeld zahlen, ist laut der Studie von Arcserve, dass nur 17 Prozent der Führungskräfte im Gesundheitswesen großes Vertrauen in die Fähigkeit ihres IT-Teams haben, verlorene Daten nach einem Angriff vollständig wiederherzustellen. Diverse Schwächen in der Strategie und in den Systemen für Datenschutz und Datensicherheit behindern die Fähigkeit, Daten in solchen Situationen schnell wiederherzustellen. Zunächst einmal verfügen viele Organisationen nicht über robuste Backup-Systeme. Falls doch, werden diese Systeme nicht regelmäßig getestet und aktualisiert, was die Wiederherstellung bei Kompromittierung oder Verschlüsselung der Daten erschwert.

Ein weiteres Problem ist das Fehlen von Offline-Backups: Viele Organisationen im Gesundheitswesen verlassen sich ausschließlich auf Online- oder Netzwerk-Backups. Doch hierbei besteht die Gefahr, dass diese Backups von den Cyberkriminellen meist ebenfalls verschlüsselt werden. Ein weiteres Gefahrenpotenzial ist der Faktor

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Mensch: Menschliches Versagen durch Mitarbeiter, die auf bösartige Links klicken oder infizierte E-Mail-Anhänge öffnen, ist eine häufige Ursache für die Verbreitung von Ransomware. In vielen Organisationen des Gesundheitswesens mangelt es noch immer an Schulungen und Sensibilisierungsprogrammen für Mitarbeiter in Bezug auf bewährte Verfahren für die Cybersicherheit.
Hinzu kommen vielfach auch noch Budgetrestriktionen. Sie behindern Organisationen im Gesundheitswesen, eine wirksame Datensicherheit und Resilienz aufzubauen. Unzureichende finanzielle Mittel sorgen nicht nur für eine technologische Lücke, sondern auch für zu wenig Spezialisten und Ressourcen – sowohl um die Datensicherheit wesentlich zu härten als auch um mit Angriffssituationen umzugehen. Das Resultat ist ein relativ leichtes Spiel für die Cyberkriminellen, um die Lücken auszunutzen.

3-Schritte zur Ransomware-Prävention

Ein entscheidender Punkt ist, dass die Zahlung von Lösegeld keine vollständige Datenwiederherstellung oder gar den Schutz vor zukünftigen Angriffen garantiert. Die Zahlung von Lösegeld kann sogar mehr schaden als nützen, da sie künftige Ransomware-Angriffe begünstigt und zur Rentabilität und Hartnäckigkeit der Internetkriminalität insgesamt beiträgt. Was können Organisationen im Gesundheitswesen also tun? Im Folgenden werden drei Möglichkeiten beschrieben, wie Organisationen die Ransomware-Bedrohung entschärfen und sich und ihre Patienten schützen können.

1. ***Entwicklung eines umfassenden Plans für die Widerstandsfähigkeit von Daten***

Organisationen des Gesundheitswesens sollten einen klar definierten und dokumentierten Plan zur Datensicherheit erstellen, der Strategien, Richtlinien und Verfahren zum Schutz vor Ransomware-Angriffen enthält. Der Plan sollte Präventivmaßnahmen, Protokolle für die Reaktion auf Vorfälle, Datensicherungs-

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

und Wiederherstellungsprozesse sowie Strategien zur kontinuierlichen Überwachung und Verbesserung umfassen.

Organisationen sollten außerdem regelmäßig Übungen und simulierte Cyberangriffsszenarien durchführen, um die Wirksamkeit ihrer Pläne zur Datensicherheit zu testen. Diese Übungen können Lücken und Schwachstellen in den Plänen aufdecken und Anpassungen aufzeigen, die vorgenommen werden müssen.

Darüber hinaus sollten nach tatsächlichen Cybervorfällen die Wirksamkeit der Reaktion überprüft, bewertet und verbesserungswürdige Bereiche ermittelt werden. Diese Feedback-Schleife ist entscheidend für die kontinuierliche Verbesserung der Reaktionsfähigkeit einer Organisation und die Gewährleistung der Tragfähigkeit ihrer Pläne.

2. *Erhöhung der Datensicherheit durch die 3-2-1-1-Strategie mit unveränderlichem Speicher*

Eine weitere wichtige Maßnahme, die Organisationen in Betracht ziehen sollten, ist der 3-2-1-1-Ansatz für die Datensicherheit. Die Basis dieser Strategie – die 3-2-1-Regel – sieht vor, dass drei Sicherungskopien der Daten auf zwei verschiedenen Datenträgern aufbewahrt werden: beispielsweise Festplatte und Band. Darüber hinaus sollten Organisationen eine dieser Kopien außerhalb des Unternehmens aufbewahren, um die Wiederherstellung im Notfall zu erleichtern.

Die letzte, zusätzliche 1 in dieser Strategie ist entscheidend für den Schutz vor den Folgen einer Ransomware und für die schnelle Wiederherstellung: der unveränderliche Objektspeicher. Die unveränderliche Objektspeicherung ist ein fortschrittliches Werkzeug für die Datensicherheit. Es bietet kontinuierlichen Schutz, indem es alle 90 Sekunden ein Snapshot der Daten anlegt. So lassen sich die Daten

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

selbst im Katastrophenfall mühelos und je nach Zeitabstand der Snapshots mit nahezu keinem Datenverlust wiederherstellen. Unveränderliche Snapshots auf Objektspeicher können von Ransomware nicht verändert, überschrieben oder gelöscht werden. Die Snapshots ermöglichen die Datenwiederherstellung von vielen Zeitpunkten, so dass Unternehmen bei Systemausfällen, Naturkatastrophen oder Ransomware-Angriffen zu früheren Datenständen problemlos zurückkehren können.

3. Ausbildung und Schulung von Mitarbeitern

Das schwächste Glied in der Sicherheit ist oft der Benutzer. Aus diesem Grund sollten Organisationen im Gesundheitswesen regelmäßig Schulungsprogramme zur Cybersicherheit für alle Mitarbeiter durchführen. Diese Programme sollten die mit Ransomware-Angriffen verbundenen Risiken hervorheben und Richtlinien für bewährte Verfahren enthalten. Die Mitarbeiter sollten darin geschult werden, Phishing-E-Mails, verdächtige Links und andere potenzielle Quellen von Malware zu erkennen, um mögliche Infektionen und Angriffe zu verhindern.

Programme zur Sensibilisierung für Cybersicherheit rüsten die Mitarbeiter mit dem notwendigen Wissen und den Werkzeugen aus, um aktiv zur Sicherheitslage der Organisation beizutragen. Wenn sie sich mit den besten Praktiken vertraut machen, werden die Mitarbeiter zu einer wichtigen Verteidigungslinie gegen Cyber-Bedrohungen. Durch kontinuierliche Schulungen können Gesundheitsorganisationen eine Kultur der Wachsamkeit fördern und sicherstellen, dass alle Mitarbeiter ihre Rolle bei der Aufrechterhaltung einer robusten Cybersicherheit verstehen.

Fazit

Indem sie ihre Strategien zur Datensicherheit an den drei genannten Aspekten ausrichten, können Organisationen des Gesundheitswesens die Gefährdung durch Ransomware-Angriffe minimieren und im Idealfall Lösegeldzahlungen vermeiden.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Noch besser: Die Organisationen können ihre kritischen Daten schützen, die Kontinuität der Versorgung aufrechterhalten und die höchsten Standards für die Patientensicherheit einhalten.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

Über Arcserve

Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der vier Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt. Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf X oder LinkedIn.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de