arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

6 Schritte für mehr Cyber-Resilienz im Gesundheitswesen

Krankenhäuser und Pflegeeinrichtungen werden häufig zum Ziel von Cyberattacken. Besonders bedenklich in diesem Zusammenhang ist, dass sich laut einer internationalen Studie die Wiederherstellungskosten bei Ransomware-Attacken im Gesundheitssektor deutlich erhöht haben. Mit durchschnittlich über 2 Millionen Euro (2,2 Millionen US-Dollar) mussten Healthcare-Unternehmen 2023 deutlich tiefer in die Tasche greifen, um wieder betriebsfähig zu werden. In 2021 reichten noch 1,1 Millionen Euro (1,27 Millionen US-Dollar) aus. Innerhalb von zwei Jahren haben sich die Wiederherstellungskosten also fast verdoppelt. Das zeigt, dass Attacken zunehmend „professionell" durchgeführt werden und dass die Einrichtungen nicht genügend vorbereitet sind. Es ist daher nur eine Frage der Zeit, bis ein Cyberangriff eine Gesundheitseinrichtung lahmlegt und neben der potenziellen Betriebsunfähigkeit auch für immens hohe Kosten sorgt. Dabei ließe sich schon mit diesen sechs Tipps die Schlimmste verhindern.

1. Risikobewertung und -management

Eine gründliche Risikobewertung kann helfen, Schwachstellen in den IT-Systemen des Gesundheitswesens zu ermitteln. Bei der Bewertung müssen alle potenziellen Angriffspunkte für Ransomware berücksichtigt werden, einschließlich der Geräte von Mitarbeitern, Überwachungsgeräte, Fernzugriffssysteme und Dienste von Drittanbietern.

2. Mitarbeiterschulung und Sensibilisierungsprogramme

Der Verizon Data Breach Investigations Report (DBIR) fand heraus, dass bei 68 Prozent der Datenschutzverletzungen menschliches Versagen im Spiel war, inkl. Social Engineering. Immer wieder warnen Fachleute davor, dass Hacker die gestohlenen Identitäten von Mitarbeitern nutzen, um Angriffe auf

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

die IT-Abteilungen von Krankenhäusern zu starten. Awareness-Programme könne helfen, die Mitarbeiter zu sensibilisieren.

3. Umfassende Pläne zur Datensicherung und Notfallwiederherstellung
Die Vorbereitung auf den Katastrophenfall ist für die Wiederherstellung nach einer Ransomware-Attacke oder einem Cyberangriffen unerlässlich. Leitfäden mit einer "Schritt-für-Schritt-Anleitung zur Erstellung eines Disaster-Recovery-Plans" können helfen, sich auf den Worst-Case vorzubereiten.

4. Netzwerksicherheit verbessern (inkl. IoT-Cybersecurity)
Erweiterte Netzwerkschutzmaßnahmen sind wichtiger denn je. Das NIST Cybersecurity Framework bietet Schnellstartanleitungen, Ressourcen und Vorlagen, die Einrichtungen bei der Implementierung effektiver Lösungen unterstützen. Dazu sollten sowohl Intrusion Detection Systeme (IDS) als auch Endpunktschutzplattformen gehören, die Bedrohungen in Echtzeit erkennen und darauf reagieren können.

5. Planung und Durchführung von Worst-Case-Szenarien
Es empfiehlt sich einen Reaktionsplan für kritische Zwischenfälle zu entwickeln, der speziell auf das Gesundheitswesen zugeschnitten ist. Dieses Konzept muss klare Rollen, Verantwortlichkeiten, Reaktionsverfahren und Kommunikationsstrategien enthalten. Mehr Informationen dazu in "Wie man auf eine Katastrophe reagiert".

6. Einsatz einer einheitlichen Datensicherungsplattform
Da in Unternehmen Daten über verschiedene Einrichtungen, Speichermedien und Anwendungen verteilt sein können, kann eine einheitliche Backup-Lösung die Folgen eines Cyberangriffs abmildern. Der Einsatz von Lösungen, welche die IT-Resilienz erhöhen, indem sie Prozesse auf allen Speicherplattformen – lokal, virtuell oder in der Cloud – vereinfacht, sind am effektivsten.

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Grundsätzlich gilt: Anzufangen ist besser als zu warten, bis alles perfekt ist. Vor allem aber geht es darum das Bewusstsein der Mitarbeiter zu schärfen, denn leider gehört deren sorgloser Umgang mit den digitalen Informationen und Daten zu den häufigsten Ursachen, dass Hacker ihre Ziele erreichen.

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

###

Über Arcserve

Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt
Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
arcserve@tc-communications.de