Acronis

Fünf Schritte zum Aufbau von Cyber-Resilienz im Gesundheitswesen

Das Gesundheitswesen ist ein lukratives Ziel für groß angelegte Cyberangriffe, und die Kosten für die Schadensbehebung steigen jedes Jahr in zweistelliger Milliardenhöhe. Warum steigen die Kosten für die Datenwiederherstellung? Die heutigen Gesundheitssysteme sind stark vernetzt, was die Auswirkungen und Schäden von Angriffen noch verstärkt. Cyberkriminelle können in kürzerer Zeit und mit weniger Ressourcen mehr Schaden anrichten.

Von der Vorstandsetage bis zum OP-Tisch: Ausfallzeiten betreffen alle Bereiche des Gesundheitswesens

92 %
der Gesundheitseinrichtungen haben im Jahr 2024 mindestens einen Angriff gemeldet.[1]

300 %
mehr Ransomware-Angriffe im Gesundheitssektor seit 2015.[2]

41 %
der CISOs nennen Ransomware als eine der drei größten Bedrohungen.[3]

56 %
der Gesundheitseinrichtungen berichten über schlechte Patientenergebnisse aufgrund von Angriffen.[4]

53 %
der Gesundheitseinrichtungen beobachteten eine Zunahme medizinischer Komplikationen aufgrund von Angriffen.[5]

28 %
der Gesundheitseinrichtungen, die von Cyberangriffen betroffen waren, berichten von einem Anstieg der Sterblichkeitsrate.[6]

Fünf Schritte zum Aufbau von Cyber-Resilienz im Gesundheitswesen: Abwehr und Wiederherstellung

Zuverlässige Cybersicherheit zur Priorität machen

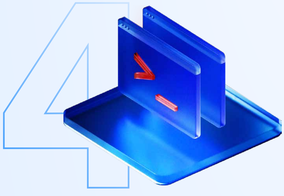
Investieren Sie in moderne Lösungen, die Bedrohungen erkennen, ihnen vorbeugen und auf sie reagieren. Aktualisieren Sie Ihre Software regelmäßig und patchen Sie Schwachstellen umgehend.

Einführung einer starken Segmentierung

Beschränken Sie die laterale Ausbreitung von Eindringlingen in Ihrem Netzwerk. Isolieren Sie kritische Systeme, um großflächige Ausfälle zu verhindern.

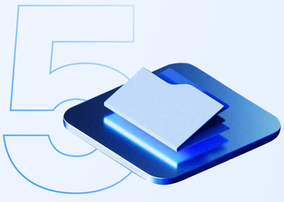
Entwicklung von Business Continuity- und Disaster Recovery-Plänen

Stellen Sie mit gut getesteten Plänen sicher, dass der Geschäftsbetrieb nach einem Angriff fortgesetzt oder schnell wiederhergestellt werden kann.



Drittanbieter-Risikomanagement stärken

Überprüfen Sie die Sicherheitspraktiken aller Zulieferer und Partner gründlich und überwachen Sie diese kontinuierlich, insbesondere diejenigen mit umfassendem Zugriff auf das System.



Verbesserung der Reaktionsfähigkeiten bei Zwischenfällen

Erstellen Sie klare Protokolle mit Maßnahmen zur Erkennung, Eindämmung und Behebung von Cybervorfällen. Führen Sie regelmäßig Simulationen und Schulungen durch.

Weitere Informationen zu Acronis Cyber Protect für das Gesundheitswesen

↘ Mehr erfahren

[1] **The HIPAA Journal. „92% of U.S. Healthcare Organizations Experienced a Cyberattack in the Past Year." Veröffentlicht am 9. Oktober 2024.** https://www.hipaajournal.com/92pc-us-healthcare-organizations-cyberattack-past-year/

[2] **IBM. „When ransomware kills: Attacks on healthcare facilities." Veröffentlicht am 30. Januar 2025.** https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities

[3] **Statista. „Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISOs) as of February 2024." Veröffentlicht am 10. März 2025.** https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

[4, 5, 6] **„Nearly 70% of healthcare organizations hit by cyberattacks report patient care disruptions: survey." Veröffentlicht am 8. Oktober 2024.** https://www.healthcaredive.com/news/healthcare-cyberattacks-patient-care-disruption-ponemon-proofpoint-survey/729251/