Acronis

Cinque passaggi per la resilienza digitale del settore sanitario

Il settore sanitario è tra le destinazioni più appetibili e redditizie degli attacchi informatici su vasta scala; i costi di ripristino crescono a dismisura e ammontano a decine di miliardi di dollari ogni anno. Perché i costi di ripristino continuano ad aumentare? Gli attuali ecosistemi sanitari sono fortemente interconnessi e questo non fa che amplificare l'impatto e i danni degli attacchi. Per produrre danni ancora più gravi, i cybercriminali possono usare meno tempo e risorse.

Dalla sala riunioni alla sala operatoria: nel settore sanitario le conseguenze di un'interruzione colpiscono tutti

92%
è la percentuale di organizzazioni sanitarie che ha subito almeno un attacco nel 2024.[1]

300%
è la percentuale di attacchi ransomware che ha colpito il settore sanitario dal 2015.[2]

41%
è la percentuale di CISO che indica il ransomware come una delle tre principali minacce.[3]

56%
è la percentuale di organizzazioni sanitarie che riferisce decorsi con esito negativo per i pazienti in seguito agli attacchi.[4]

53%
è la percentuale di organizzazioni sanitarie che ha registrato un aumento delle complicazioni mediche in seguito a un attacco.[5]

28%
è la percentuale di organizzazioni sanitarie colpite da attacchi che segnala un aumento dei tassi di mortalità.[6]

Cinque passaggi per la resilienza digitale del settore sanitario: difesa e ripristino

1

Priorità alle misure di Cyber Security consolidate

Investi in funzionalità di rilevamento, prevenzione e risposta agli attacchi avanzati. Aggiorna regolarmente il software e applica tempestivamente le patch alle vulnerabilità.

2

Segmentazione rafforzata

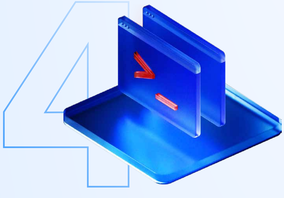
Limita il movimento laterale degli attaccanti nella rete. Isola i sistemi critici per evitare che le interruzioni operative si estendano.

3

Piani di continuità operativa e disaster recovery

Predisponi piani collaudati per garantire la continuità delle operazioni aziendali e il ripristino rapido dopo un attacco.

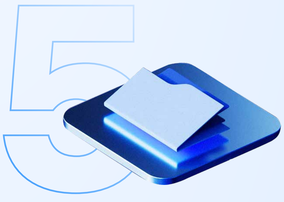
4



Gestione rafforzata dei rischi di terze parti

Esamina e monitora costantemente le procedure di sicurezza di tutti i fornitori e partner, soprattutto per quelli che hanno ampio accesso ai sistemi.

5



Capacità di incident response migliorate

Definisci protocolli chiari per l'identificazione, il contenimento e il recupero dopo un incidente informatico. Svolgi regolarmente simulazioni e attività di formazione.

Scopri di più su Acronis Cyber Protect per il settore sanitario

↘ Scopri di più

[1] **HIPAA Journal: "Il 92% delle organizzazioni sanitarie statunitensi ha subito un attacco informatico nel corso dell'ultimo anno", pubblicato il 9 ottobre 2024.** https://www.hipaajournal.com/92pc-us-healthcare-organizations-cyberattack-past-year/

[2] **IBM: "Quando il ransomware uccide: gli attacchi alle strutture sanitarie", pubblicato il 30 gennaio 2025.** https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities

[3] **Statista. "Le più significative minacce alla sicurezza informatica nelle organizzazioni globali, secondo i CISO. Febbraio 2024", pubblicato il 10 marzo 2025.** https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

[4, 5, 6] **Healthcare Dive. "Quasi il 70% delle organizzazioni sanitarie colpite da cyberattacchi segnala conseguenti interruzioni dei servizi offerti ai pazienti: un'indagine", pubblicato l'8 ottobre 2024.** https://www.healthcaredive.com/news/healthcare-cyberattacks-patient-care-disruption-ponemon-proofpoint-survey/729251/