Acronis

Soluzioni di cyber protection per le sfide del XXI secolo del settore Healthcare

Strumenti per la protezione dei dati sensibili destinati ai team IT del settore Healthcare, per affrontare le minacce informatiche della nuova era.

Il passaggio dai metodi antiquati di archiviazione delle informazioni dei pazienti all'adozione di nuove applicazioni ad utilizzo intensivo dei dati per la cura e la diagnosi caratterizza la cruciale trasformazione digitale che vede protagonista il settore Healthcare. In parallelo, sulle strutture dell'Healthcare grava un'enorme pressione a incrementare i profitti, conformarsi alle norme sulla privacy, ottimizzare le cure offerte ai pazienti e rendere più efficiente l'interazione con contribuenti, fornitori, distributori, istituzioni accademiche e pazienti.

Cresce intanto il volume dei dati costituito dalle informazioni sanitarie sensibili, che di pari passo si diffonde su posizioni fisiche, dispositivi informatici e reti, inclusi i cloud pubblici e privati. All'abbondanza dei dati contribuiscono le più recenti applicazioni del settore, come la telemedicina, il monitoraggio da remoto dei pazienti e la formazione basata su ambienti virtuali o sulla realtà assistita. A complicare il puzzle si aggiungono tecnologie emergenti come l'intelligenza artificiale, l'apprendimento automatico, l'Internet of Things (IoT), la blockchain e la richiesta di accesso ai dati proveniente da un numero sempre più alto di utenti.

Al contempo, il settore subisce l'assalto delle più recenti minacce informatiche, con violazioni della privacy, attacchi ransomware e campagne di cryptojacking. In breve, cercare di mantenere la disponibilità, l'accessibilità e la privacy dei dati nel settore Healthcare non è mai stato così complicato.

Il comparto è da tempo bersaglio di criminali informatici e attori istituzionali ostili, che sfruttano la particolare efficacia degli attacchi di malware, come il ransomware, quando l'accesso ai dati sensibili può essere una questione di vita o di morte.

Si spiega così l'ondata di attacchi ransomware di alto profilo perpetrati negli ultimi anni ai danni delle strutture dell'Healthcare; ad essere colpiti, tra gli altri, il Servizio Sanitario Nazionale del Regno Unito, Hancock Health, Adams Memorial Hospital, MedStar Health, Erie County Medical. Le violazioni dei dati nel settore occupano regolarmente i titoli dei quotidiani: ogni anno gli hacker si appropriano di centinaia di milioni di cartelle cliniche e registrazioni di pagamenti.

Il settore è inoltre nel mirino delle autorità di controllo della compliance che si occupano delle normative sulla privacy, quali HIPAA (Health Insurance Portability and Accountability Act) negli Stati Uniti, il GDPR (Regolamento generale sulla protezione dei dati) dell'Unione Europea e le normative a livello di singolo stato negli USA, come il CCPA (California Consumer Privacy Act). Gli attori del settore devono inoltre prestare attenzione al rischio di violazione degli standard normativi in materia d'uso delle carte di credito, come il PCI DSS (Payment Card Industry Data Security Standard).

Copyright © 2002-2019 Acronis International GmbH.

L'impiego delle cartelle cliniche elettroniche dei pazienti ha accresciuto l'importanza della disponibilità ininterrotta dei dati. I tempi di fermo, oltre a essere un'ovvia minaccia alla sicurezza dei pazienti, possono rivelarsi costosi al punto da mettere a rischio la solvenza stessa degli istituti del settore della santità. Secondo lo studio di Gartner "Downtime Cost Calculator for Data Center Disaster Recovery Planning", pubblicato il 28 febbraio del 2014, il costo medio dei tempi di fermo per qualsiasi attività ammonta a 5.600 dollari al minuto, pari a circa 300.000 dollari l'ora. Information Technology Intelligence Consulting conclude che **per il 98% delle aziende, una sola ora di fermo ha un costo superiore ai 100.000 dollari, che sale da 1 a 5 milioni di dollari per le aziende di maggiori dimensioni.**

Oltre a questi ostacoli specifici, i team IT nelle istituzioni dell'Healthcare devono affrontare le stesse sfide che affliggono tutti gli altri settori: complessità crescente delle infrastrutture, difficoltà di reclutare e trattenere in azienda personale qualificato, migrazione costante delle applicazioni verso cloud pubblici e privati, proliferazione di dispositivi mobile come smartphone e tablet, avvento dei sensori IoT, dispositivi di tracciamento delle risorse, fotocamere web e la necessità di effettuare analisi in tempo reale sui nuovi dati acquisiti.

Sopravvivere di fronte a queste sfide implica l'adozione di un nuovo approccio alla salvaguardia dei dati, che deve fondarsi sui cinque vettori della Cyber Protection:

SALVAGUARDIA

Assicurare che sia sempre disponibile una copia affidabile dei dati

ACCESSIBILITÀ

Agevolare la disponibilità dei dati ovunque e in qualsiasi momento

PRIVACY

Controllare chi può visualizzare e accedere ai dati

AUTENTICITÀ

Dimostrare in modo incontrovertibile che una copia è una replica esatta dell'originale

SICUREZZA

Proteggere i dati, le app e i sistemi dalle minacce

Questo white paper esamina i principi fondamentali della cyber protection a fronte delle sette sfide critiche per il settore Healthcare:

1. **Affrontare** le violazioni dei dati
2. **Proteggere** da minacce malware quali ransomware e cryptojacking
3. **Rispettare** i requisiti di conformità
4. **Migrare** applicazioni e storage critici su cloud pubblici e privati
5. **Assicurare** la disponibilità ininterrotta dei dati
6. **Integrare** i dispositivi mobile nell'organizzazione
7. **Consolidare** la protezione dei dati senza aggiungere complessità infrastrutturali

Copyright © 2002-2019 Acronis International GmbH.

L'IT DEL SETTORE HEALTHCARE: LO STATO DELL'ARTE

La protezione e la sicurezza dei dati sono imprescindibili nelle odierne strutture dell'Healthcare. In una ricerca sulle violazioni dei dati, Protenus, società che si occupa di sicurezza informatica, ha segnalato che nel 2017 è stato registrato più di un attacco al giorno nel settore Healthcare.

Sempre nel 2017, sono state violate 5,6 milioni di cartelle cliniche, con una media di 308 giorni necessari per scoprire l'avvenuta violazione.

Per limitare il numero di violazioni dei dati nel settore, sono necessari più livelli di sicurezza dell'infrastruttura IT, da disporre intorno ai sistemi fisici, alle macchine virtuali, ai servizi cloud e ai dispositivi mobile. Le contromisure di base includono la protezione anti-malware sugli endpoint, la difesa mediante firewall dalle minacce provenienti dall'esterno della rete e la segmentazione della rete tramite vLAN o reti software-defined, per limitare la diffusione degli attacchi sulle reti interne. La protezione dei dati con backup e disaster recovery è fondamentale nel caso in cui un attacco danneggi, distrugga o impedisca l'accesso ai dati riservati. Per implementarla è necessario disporre di sistemi di archiviazione e backup protetti e crittografati, sia in sede che nel cloud.

LE MINACCE MALWARE

Secondo la maggior parte delle ricerche sulla sicurezza, le due minacce malware più insidiose che negli ultimi anni bersagliano il settore Healthcare sono il ransomware e il cryptojacking.

Il primo attacca server, desktop e dispositivi mobile (in genere perché un utente apre un link o un allegato dannoso contenuto in un'email di phishing), crittografa tutti i dati che questi contengono e richiede quindi un pagamento online in cambio della chiave di decrittografia necessaria per sbloccare i file della vittima. Non disponendo di contromisure volte a individuare e arrestare gli attacchi ransomware, né di capacità di eseguire il ripristino a partire da backup recenti, molte istituzioni dell'Healthcare hanno registrato tempi di fermo che hanno messo a repentaglio la vita dei pazienti e hanno avuto costi nell'ordine di milioni di dollari, in perdite di produttività e spese di riparazione.

Il cryptojacking è un tipo di attacco meno esplicito ma in costante diffusione, che trasforma i sistemi infettati del sistema dell'Healthcare in una sorta di zombie all'interno di botnet sfruttate per il mining delle criptovalute per conto dei criminali informatici. Alle vittime, il malware ruba soltanto risorse (processi di elaborazione, memoria, elettricità, energia per il raffreddamento) ma i sistemi subiscono danni in termini di costi energetici e usura. Inoltre, il cryptojacking inietta spesso altre minacce, come il ransomware, nei sistemi che infetta.

REQUISITI DI CONFORMITÀ

Il controllo normativo esercitato sul settore Healthcare ha contribuito a renderlo uno dei bersagli preferiti da parte dei criminali che diffondono malware quale il ransomware. Il rischio di subire violazioni della conformità causate dal ransomware, che blocca i dati sensibili dei pazienti, spinge le vittime a pagare il riscatto per recuperare l'accesso ai dati.

Per il secondo anno di fila, agli attacchi ransomware va imputato **il 70% di tutti gli incidenti causati dal malware nel settore Healthcare,** secondo quanto si legge nel rapporto di Verizon "Data Breach Investigations Report" per il 2019.

MIGRAZIONE NEL CLOUD DI APPLICAZIONI E STORAGE

Come per la maggior parte dei settori, anche quello sanitario sta affrontando il lungo percorso di migrazione delle applicazioni e dei dati critici su infrastrutture che combinano cloud pubblico e privato. L'obiettivo è ridurre i costi, sostituire le spese di capitale con quelle per servizi prevedibili e migliorare l'accessibilità e la condivisione dei dati da qualsiasi posizione o dispositivo. Molte istituzioni sono tuttavia alle prese con la difficoltà di spostare in sicurezza nel cloud le risorse destinate alla protezione dei dati e allo storage, mantenendo al tempo stesso la privacy dei dati e rispettando le normative sulla compliance.

Per il secondo anno di fila, agli attacchi ransomware va imputato il 70% di tutti gli incidenti causati dal malware nel settore Healthcare, secondo quanto si legge nel rapporto di Verizon "Data Breach Investigations Report" per il 2019.

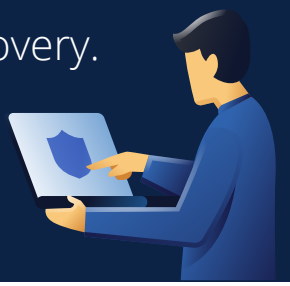
Copyright © 2002-2019 Acronis International GmbH.

DISPONIBILITÀ DEI DATI

Il settore Healthcare ha ovvie motivazioni per perseguire la disponibilità continua e ininterrotta dei dati, da cui spesso dipende la salute e la sopravvivenza dei pazienti.

Dal punto di vista del backup e del ripristino, ciò richiede che i professionisti IT prestino particolare attenzione a due parametri: gli obiettivi di punto di ripristino (RPO) e di tempo di ripristino (RTO). Il primo definisce quante informazioni l'azienda può permettersi di perdere in un determinato momento e corrisponde alla frequenza con cui dovrà creare il backup dei dati critici. Il secondo riflette il tempo massimo di inattività che un'istituzione può sostenere tra il verificarsi di un eventuale guasto dei sistemi e il ripristino degli stessi. La maggior parte delle istituzioni può identificare con facilità le applicazioni che richiedono RPO e RTO più rigidi e quali possono sostenere perdite di dati più rilevanti e tempi di ripristino più lunghi.

Acronis offre alle istituzioni dell'Healthcare un set di soluzioni facili da usare, estremamente flessibili e integrate per la cyber protection, l'archiviazione e il disaster recovery.



I RISCHI DEL BYOD

L'avvento dell'uso dei dispositivi di proprietà dei dipendenti nel settore Healthcare ha portato numerosi vantaggi al comparto, inclusa una maggiore produttività e collaborazione del personale. Ha tuttavia aggiunto anche difficoltà nella protezione dei dati, perché aumenta la possibilità che i dati sensibili vengano memorizzati su dispositivi facili da manomettere, rubare o smarrire.

SEMPLIFICAZIONE DELLA CYBER PROTECTION

Come in molti altri settori, anche i responsabili IT della sanità faticano a reclutare professionisti qualificati, di conseguenza è assolutamente fondamentale ridurre il più possibile la complessità delle operazioni. Questo aspetto è particolarmente rilevante rispetto ai problemi operativi di routine, come la protezione dei dati. L'adozione di più sistemi per gestire un ambiente IT diversificato, con la conseguente necessità di reperire tecnici altamente qualificati per controllarlo, non è certo la scelta ottimale.

LE SOLUZIONI DI CYBER PROTECTION ACRONIS PER IL SETTORE HEALTHCARE

Acronis protegge dalle violazioni dei dati con diverse soluzioni. Acronis Cyber Backup applica la crittografia ai dati sensibili a riposo e in transito, per garantire che anche nel caso in cui le misure difensive vengano superate, i criminali non possano sfruttare a proprio vantaggio le informazioni che hanno danneggiato.

La soluzione consente anche di ripristinare completamente i dati manomessi, distrutti o bloccati da un attacco informatico.

Acronis Cyber Cloud Storage protegge dati e backup dalle violazioni con una straordinaria gamma di difese informatiche, inclusa la crittografia avanzata dei dati e dei backup (a riposo e in transito) e data center in cloud protetti e certificati.

PROTEGGERE DA MINACCE MALWARE COME IL RANSOMWARE E IL CRYPTOJACKING

Acronis Cyber Backup con Acronis Active Protection adotta tecnologie di intelligenza artificiale e machine learning per individuare, bloccare e invertire le modifiche sospette a dati, file e agenti di backup, utilizzando la cache per annullare i cambiamenti apportati.

La soluzione rileva e blocca automaticamente gli attacchi di cryptojacking, offrendo pertanto una difesa senza pari contro due delle minacce malware più insidiose per il settore Healthcare; le contromisure già esistenti, quali software antivirus basati su firme, vengono così completate dalle difese contro le minacce di tipo zero-day.

Acronis Cyber Backup rafforza inoltre l'agente e gli archivi di backup contro gli attacchi malware, impedendo che un'eventuale violazione possa compromettere la capacità dell'istituzione di recuperare prontamente e tornare alla normale operatività.

Copyright © 2002-2019 Acronis International GmbH.

RISPETTARE I REQUISITI DI CONFORMITÀ

Le funzionalità di crittografia di Acronis Cyber Backup con Acronis Active Protection e Acronis Cyber Cloud Storage supportano anche gli obiettivi di conformità, poiché proteggono la privacy delle informazioni sanitarie sensibili rendendole inutili per i criminali informatici anche in caso di successo della violazione. I prodotti Acronis sono dotati di molte altre funzioni e caratteristiche native, che, quando configurate e utilizzate adeguatamente, assicurano la conformità con le sezioni applicabili della normativa HIPAA e HITECH (Health Information Technology for Economic and Clinical Health Act) del 2009. Benché non sussista alcun accreditamento o processo di certificazione legalmente riconosciuto per HIPAA o HITECH, **il programma di sicurezza e conformità di Acronis è progettato per ridurre al minimo i problemi di conformità con le due normative.** Per altre informazioni, visitate Acronis Resource Center.

MIGRARE APPLICAZIONI E STORAGE CRITICI SU CLOUD PUBBLICI E PRIVATI

Acronis Cyber Backup semplifica il processo di migrazione delle applicazioni del sistema dell'Healthcare verso il cloud, supportando una vasta serie di servizi cloud, sistemi operativi (fisici e virtuali), carichi di lavoro applicativi (on-premise e nel cloud) ed endpoint. Il ventaglio di strumenti di gestione di Acronis Cyber Backup rende semplice e sicuro il trasferimento dei carichi di lavoro tra ambienti fisici, virtuali e cloud, accelerando la migrazione senza rischi verso nuove piattaforme, quali cloud privati, Acronis Cyber Cloud Storage e le offerte di cloud pubblico più diffuse: Amazon, Google e Microsoft.

ASSICURARE LA DISPONIBILITÀ ININTERROTTA DEI DATI

Acronis Cyber Backup offre alle istituzioni dell'Healthcare funzionalità utili per agevolare in modo intelligente la gestione degli obiettivi RTO e RPO nei propri ambienti applicativi.

1. Acronis Instant Restore offre RTO e RPO prossimi allo zero per le applicazioni più importanti.
2. Acronis Universal Restore fornisce grande flessibilità per il ripristino di un sistema su un nuovo hardware bare-metal o su una diversa piattaforma, ad esempio da una macchina virtuale fisica a una virtuale, in caso di necessità.
3. Acronis Active Protection è una funzione integrata che elimina i tempi di fermo e la perdita di prestazioni associati agli attacchi ransomware e di cryptojacking.

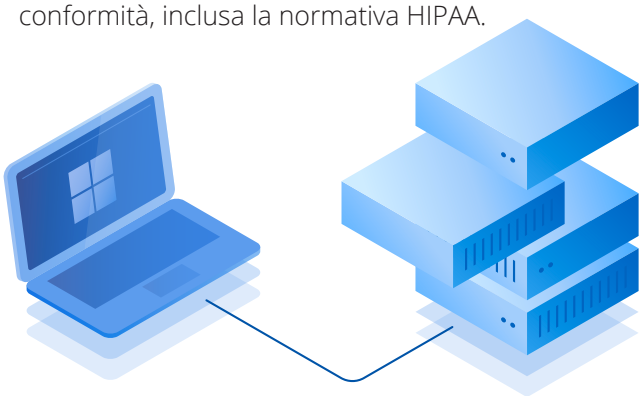
PROTEGGERE I DATI SENSIBILI SU OGNI DISPOSITIVO

Acronis Files Advanced aiuta a migliorare l'assistenza al paziente e l'efficienza operativa, garantendo al tempo stesso l'adesione ai più severi standard di sicurezza e conformità, inclusa la normativa HIPAA. Il prodotto consente a dipendenti, partner e subappaltatori del settore Healthcare di condividere e collaborare su documenti riservati. Alle istituzioni è comunque garantito il mantenimento del controllo completo su posizione, gestione e privacy dei dati.

Il policy engine di Acronis Files Advanced offre funzioni di gestione capillare per assicurare controllo e conformità di contenuti, utenti e dispositivi. La soluzione garantisce anche la protezione e la riservatezza totale delle informazioni, grazie alla crittografia dei dati a riposo e in transito. Inoltre, implementando controlli delle policy centralizzati, Acronis Files Advanced consente ai team IT di prevenire la perdita di informazioni, le violazioni della condivisione dei dati e le violazioni della sicurezza.

Fornitori di servizi Healthcare, studi medici e pazienti utilizzano Acronis Files Advanced per l'accesso, la modifica, la creazione e la condivisione dei dati sanitari con qualsiasi dispositivo: desktop, laptop, tablet o smartphone. Inoltre, gli studi medici possono adottare la soluzione con le seguenti finalità:

- **Proteggere** sia i dati sensibili dei pazienti sia i documenti amministrativi, quali informazioni riservate e ricerche, contratti accademici e aziendali e così via.
- **Fornire** a medici, ricercatori e amministratori dell'Healthcare l'accesso protetto ai dati sanitari e consentirne la facile condivisione da qualsiasi dispositivo.
- **Proteggere** i dati clinici dei pazienti, a riposo e in transito.
- **Collaborare** in modo rapido ed efficiente per offrire una migliore assistenza al paziente, sia all'interno dell'organizzazione Healthcare sia all'esterno, con i partner.
- **Tenere traccia** delle attività di accesso e condivisione dei file.
- **Rispettare** i più rigidi requisiti e standard di conformità, inclusa la normativa HIPAA.



Copyright © 2002-2019 Acronis International GmbH.

CONSOLIDARE LA PROTEZIONE DEI DATI SENZA AGGIUNGERE COMPLESSITÀ INFRASTRUTTURALI

Acronis Cyber Backup semplifica le attività di protezione informatica e ne riduce il costo rendendo disponibile una piattaforma unica capace di proteggere tutti i carichi di lavoro di un'istituzione dell'Healthcare.

È infatti in grado di gestire operazioni di archiviazione, conservazione, backup e ripristino da un unico pannello di comando, su piattaforme cloud, virtuali, fisiche e mobile, oltre ai carichi di lavoro più diffusi di Microsoft, Oracle, Google e altri. L'interfaccia e gli strumenti di monitoraggio potenti e intuitivi consentono l'uso del prodotto anche al personale meno esperto, permettendo a quello più esperto di dedicarsi ai progetti strategici.

Infine, Acronis Disaster Recovery Add-On è un'estensione semplice e di facile utilizzo di Acronis Cyber Backup. Le istituzioni dell'Healthcare possono eseguire ripristini istantanei dopo guasti dei sistemi IT, delle applicazioni e dei dati critici, attivando automaticamente i backup sulle macchine virtuali eseguite nell'ambiente di Acronis Cloud. La soluzione permette il failover di un'ampia gamma di piattaforme di elaborazione e applicazioni tra cui Windows Server, Linux, piattaforme di virtualizzazione quali VMware, Hyper-V, KVM, XenServer e Red Hat Virtualization e applicazioni Microsoft come Exchange, SQL Server, SharePoint e Active Directory.

L'ESCLUSIVA ARCHITETTURA CLOUD DI ACRONIS VI GARANTISCE IL CONTROLLO DEI DATI

QUALSIASI TIPO DI GESTIONE

Software di gestione implementato e controllato in modo indipendente: la protezione dei dati è controllata dal cliente, dal service provider, dal fornitore, dal partner o da terzi da cloud pubblico/del partner/privato o dalla sede del cliente

QUALSIASI PROTEZIONE

- Backup
- Archiviazione
- Disaster recovery
- Sincronizzazione e condivisione
- Notary/ASign
- Protezione dal ransomware

QUALSIASI CARICO DI LAVORO

- On-premise
- Cloud privato
- Cloud
- Mobile
- Applicazioni
- File
- Virtuale

QUALSIASI STORAGE

- Disco, nastro
- NAS, SAN
- Cloud del partner
- Cloud privato
- Cloud pubblico
- Acronis Cloud

QUALSIASI DEPLOYMENT

- Locale
- Cloud privato
- Cloud del partner
- Acronis Cloud
- Cloud pubblico

QUALSIASI RIPRISTINO

- Fisico
- Virtuale
- Mobile
- Applicazioni
- File
- Cloud

Copyright © 2002-2019 Acronis International GmbH.

CONCLUSIONI

Trasformazione digitale accelerata, volumi di dati in espansione, esigenze di interoperabilità crescenti e controlli più serrati da parte di azionisti e organismi di regolamentazione complicano il panorama del settore Healthcare. Trovare il giusto equilibrio nel garantire simultaneamente salvaguardia, accessibilità, privacy, autenticità e sicurezza dei dati è un compito delicato, soprattutto quando si deve far fronte anche a un esercito di criminali informatici determinati ad appropriarsi dei dati sanitari per ottenere in cambio un riscatto. Alle istituzioni dell'Healthcare si chiede oggi di rendere disponibili nuove applicazioni complesse, ridurre i costi e migliorare l'assistenza erogata ai pazienti; oltre a queste sfide specifiche del settore, esse sono tenute ad affrontare anche quelle informatiche: fidelizzazione del personale qualificato, migrazione al cloud e proliferare di dispositivi mobile e IoT.

Acronis può aiutarvi ad affrontare queste sfide con un ventaglio collaudato di soluzioni di cyber protection, archiviazione, sincronizzazione e condivisione sicure dei file e disaster recovery, ottimizzate per il settore Healthcare.

Scoprite i vantaggi che le soluzioni di Cyber Protection di Acronis hanno già offerto a una struttura Healthcare statunitense qui.

Richiedete una versione di prova gratuita **valida 30 giorni dei prodotti Acronis** per il settore Healthcare qui:

- Acronis Cyber Backup con Acronis Active Protection — RICHIEDI UNA VERSIONE DI PROVA GRATUITA VALIDA 30 GIORNI
- Acronis Disaster Recovery Add-On per Acronis Cyber Backup — RICHIEDI UNA VERSIONE DI PROVA GRATUITA VALIDA 30 GIORNI
- Acronis Files Advanced — RICHIEDI UNA VERSIONE DI PROVA GRATUITA VALIDA 30 GIORNI

Acronis

Per saperne di più, visitare **www.acronis.com**

Copyright © 2002-2019 Acronis International GmbH. Tutti i diritti riservati. Acronis e il logo Acronis sono marchi registrati di Acronis International GmbH negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi o marchi registrati sono proprietà dei rispettivi titolari. Soggetto a modifiche tecniche. Le immagini potrebbero non corrispondere al prodotto reale. Si declina qualsiasi responsabilità per possibili errori. 2019-10