Claros di Hach
Documento sulla sicurezza

Panoramica per i dirigenti

Claros è la soluzione Water Intelligence System di Hach®, realizzata per consentire alle aziende che operano nel settore idrico di utilizzare i dati di laboratorio e processo allo scopo di migliorare i risultati operativi, senza rischiare di compromettere la sicurezza. Claros è una singola piattaforma che include le soluzioni Hach Instrument Management, Data Management e Process Management. Hach è consapevole che, per costruire un rapporto di fiducia e offrire un servizio di alto livello, è essenziale aiutare i clienti a proteggere i dati, garantire la conformità alle normative di sicurezza e contenere i rischi potenziali. L'azienda adotta un approccio alla sicurezza incentrato sul rischio e in questo documento sono illustrate in dettaglio le varie misure e tecnologie utilizzate da Claros per proteggere i dati dei clienti.

Il documento spiega in che modo Claros aiuta i clienti a raggiungere gli obiettivi fondamentali di protezione delle informazioni, ovvero riservatezza, integrità e disponibilità. Vengono inoltre illustrati l'approccio di Hach all'architettura di sicurezza e le responsabilità dei clienti. In questo contesto, per riservatezza si intende una serie di regole che controllano l'accesso alle informazioni, per integrità si intende la precisione e l'attendibilità delle stesse, mentre per disponibilità si intende la possibilità di offrire un accesso affidabile ai contenuti da parte di utenti autorizzati.

Sommario degli argomenti trattati nel presente documento:

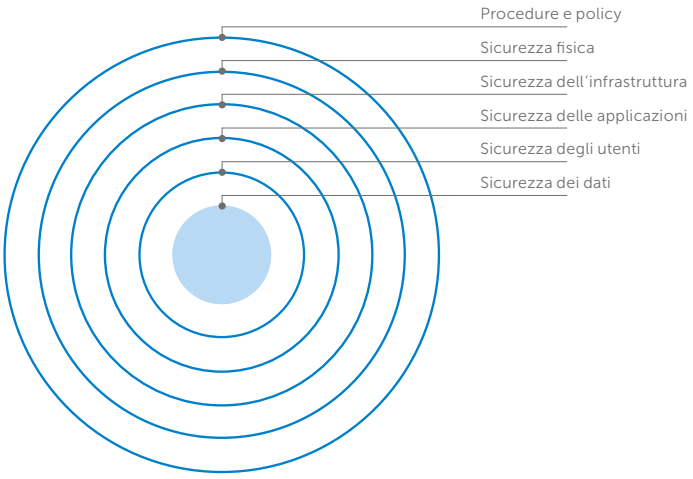
L'approccio di Hach

Defense-in-Depth (Difesa in Profondità)

Anziché offrire un singolo livello di protezione dei dati degli utenti, Claros propone una soluzione attentamente strutturata che tiene conto di ogni singolo livello, dalle misure di sicurezza fisiche nel data center fino ai privilegi di accesso che identificano i dati disponibili per i singoli utenti. Questa è infatti la strategia multistrato utilizzata da Hach per proteggere i dati dei clienti.

Per Difesa in Profondità si intende l'uso coordinato di varie contromisure di sicurezza con lo scopo di proteggere l'integrità delle risorse informative di un'azienda. Si tratta di una strategia basata sulle tattiche militari, secondo le quali superare un complicato sistema di difesa multistrato è più difficile che penetrare una barriera singola.

-TechTarget



Procedure e policy

Il primo livello di difesa è costituito da una serie di policy e processi esaustivi, chiaramente definiti per garantire la sicurezza degli utenti e dei loro dati. Il sistema di gestione della sicurezza delle informazioni (ISMS, Information Security Management System) di Hach si avvale di numerose misure basate su processi e policy, per garantire che i nostri stessi dipendenti vedano la sicurezza come una priorità assoluta.

Formazione

I dipendenti Hach autorizzati ad accedere a Claros seguono corsi di aggiornamento periodici sulle politiche di sicurezza aziendali. Ad esempio, il personale dei reparti di Sviluppo Operativo, Ricerca e Sviluppo e Supporto Tecnico e Assistenza di Hach, che può avere l'esigenza di trattare dati dei clienti e informazioni sensibili, segue regolarmente corsi di formazione su conformità e sicurezza, per essere sempre aggiornato sulle principali minacce emergenti.

Autorizzazioni di accesso

L'accesso alle aree di produzione è riservato ai soli dipendenti autorizzati. Inoltre, l'accesso operativo a Claros è consentito esclusivamente a un gruppo ristretto di dipendenti del reparto di Sviluppo Operativo di Hach. Ciò viene controllato tramite la rete aziendale Hach, per garantire che i dati siano disponibili unicamente per il personale autorizzato. Tutti i dipendenti Hach autorizzati all'accesso operativo o fisico agli ambienti di produzione, devono seguire appositi corsi di formazione e tutte le relative attività vengono registrate a scopo di audit.

Controllo delle modifiche

Il processo formale Hach per il controllo dei cambiamenti consente di minimizzare il rischio associato alle modifiche e agli aggiornamenti apportati a Claros. Non solo: rende possibile la registrazione delle modifiche di Claros e la verifica che tutti i rischi siano stati valutati, le interdipendenze analizzate e che tutte le policy e procedure necessarie siano state valutate e applicate prima di autorizzare qualsiasi cambiamento. Tutte le modifiche vengono documentate nelle Note di rilascio, che vengono distribuite ai clienti ancora prima di apportare qualsiasi aggiornamento al sistema.

Potenziamento dei sistemi

Per la fornitura del servizio, Claros utilizza numerose tecnologie attentamente coordinate, ma alcune di queste funzionalità non sono sempre necessarie. Come previsto dalle best practice di settore, il reparto Sviluppo Operativo di Claros analizza attentamente l'intera soluzione per identificare i servizi non richiesti e rimuovere e/o disabilitare tali funzionalità, allo scopo di ridurre l'esposizione alle minacce alla sicurezza.

Analisi delle vulnerabilità e pen test periodici

Conformemente alle policy interne, oltre che ai framework e agli standard internazionali di sicurezza informatica, Hach esegue periodicamente un'analisi delle vulnerabilità e penetration test incentrati sui problemi di sicurezza più critici, inclusi quelli riportati nella OWASP Top 10, per anticipare le potenziali minacce alla sicurezza.

Patch di sicurezza

Hach adotta rigorose policy e procedure per aggiornare tutti i componenti di Claros, inclusi i sistemi operativi, gli hypervisor delle macchine virtuali, il middleware, i database, le applicazioni mobili e così via con le patch di sicurezza dei relativi fornitori. Le attività associate alle patch di sicurezza sono soggette agli audit previsti dalle norme IEC62443-4-1 sul ciclo di sviluppo dei prodotti sicuri e devono rispettare standard rigorosi.

Riservatezza

Autenticazione

L'architettura Claros si avvale di un framework di sicurezza centralizzato basato su autenticazione e autorizzazione, per controllare l'accesso al servizio e ai dispositivi sul campo. Tale framework permette di applicare le misure di sicurezza tramite algoritmi di verifica che impongono l'utilizzo di password efficaci con requisiti minimi di lunghezza e complessità.

Crittografia dei dati in transito

Tutto il traffico in entrata e in uscita da Claros viene crittografato per garantire la sicurezza delle comunicazioni. A tale scopo, viene utilizzato un protocollo TLS/SSL (Transport Layer Security/Secure Sockets Layer) che sfrutta gli algoritmi SHA-2 (Secure Hash Algorithm 2) o AES (Advanced Encryption Standard) per garantire che i dati in entrata o in uscita dagli endpoint attendibili non vengano mai trasmessi in chiaro su Internet.

Crittografia dei dati archiviati

Con Hach i dati archiviati dei clienti non corrono alcun rischio. Tutti i dati di Claros vengono memorizzati nei server Microsoft Azure e codificati tramite la crittografia AES a 256 bit, allo scopo di renderli completamente illeggibili a chiunque riuscisse ad accedervi nei server.

Integrità

Accesso controllato e basato sul ruolo

L'accesso dei clienti a Claros è completamente controllato tramite interfacce utente, API (Application Programming Interface) e/o strumenti dedicati. Tutti questi metodi impongono l'utilizzo di nome utente e password con privilegi appropriati per il livello di accesso richiesto. Tutti gli amministratori Claros possono impostare le autorizzazioni degli account utente, implementando il controllo di accesso basato sul ruolo (RBAC, Role Based Access Control) in tutta l'infrastruttura Claros. In questo modo i clienti non dispongono di accesso root o amministrativo ad alcuna area dello stack tecnologico Claros e il login è consentito esclusivamente tramite il livello applicativo Claros (UI o API).

Accesso applicativo

I dati dei clienti sono accessibili esclusivamente tramite l'applicazione Claros. In ogni caso, che si utilizzino le interfacce utente o le API disponibili viene applicato il controllo dell'accesso basato sul ruolo, affinché i dati dei clienti risultino accessibili esclusivamente agli utenti autorizzati e al personale. In questo senso, Claros non consente l'accesso diretto ad alcun database. Tale approccio impedisce a servizi o sistemi non autorizzati di recuperare o modificare accidentalmente o intenzionalmente i dati dei clienti.

Comunicazione

Poiché tutte le comunicazioni con Claros vengono avviate dai dispositivi sul campo, il cliente può tracciare qualsiasi tentativo di trasmissione dalla propria rete al mondo esterno e aggiungere ulteriori misure di sicurezza alla rete circostante. Il sistema verifica l'autenticità di tutti i tentativi di comunicazione tra i dispositivi sul campo e Claros.

Firewall

Tutti gli accessi da e verso i dispositivi sul campo attraverso la rete sono protetti da un firewall multilivello impostato per impedire tutte le trasmissioni non espressamente consentite. L'accesso via Internet è permesso esclusivamente sulle porte esplicitamente aperte, e solo per un gruppo ristretto di host virtuali specificati. Per aggiungere un livello di sicurezza in più, tutti i server di database sono protetti da un firewall supplementare.

Porte e servizi non necessari

Tutti i servizi e le porte su qualunque server o dispositivo sul campo incorporato non necessari per il funzionamento di Claros vengono disabilitati, eliminando ulteriori opportunità di intrusione dall'esterno. Per utilizzare Claros è necessario aprire solo alcuni endpoint e porte all'interno della rete del cliente. Le porte e i servizi utilizzati da Claros sono riepilogati nella tabella che segue:

Porta	Direzione	Assistenza	Scopo
1194 (UDP)	Output	VPN	Accesso remoto da parte del tecnico di assistenza Hach
5671 (TCP)	Output	AMQPS	Scambio di messaggi da e verso Claros
123 (UDP)	Output	NTP	Recupera la data e l'ora correnti da un server di riferimento orario esterno
80 (TCP)	Output	HTTP	Recupera dal repository gli aggiornamenti del firmware firmati e sottoposti ad hashing
443 (TCP)	Output	HTTPS	Interfaccia utente di accesso a Claros

Disponibilità

Microsoft Azure

Claros fornisce i servizi utilizzando le tecnologie di cloud computing Microsoft Azure. Tutti i clienti Claros possono contare sullo SLA (Service Level Agreement) di Microsoft Azure, che garantisce un tempo di attività del 99,95% o superiore per tutti i principali servizi Azure.

Infrastruttura

L'infrastruttura che supporta la nostra soluzione si trova fra il livello del data center fisico e quello dell'applicazione Claros. Tale infrastruttura garantisce la sicurezza in maniera integrale ed esaustiva, per migliorare la protezione dei dati dei clienti.

Conformità

Allo scopo di aiutare i clienti a rispettare i requisiti nazionali, regionali e settoriali che disciplinano la raccolta e l'utilizzo dei dati personali, Microsoft Azure fornisce un set di offerte per la conformità più completo di qualsiasi altro fornitore di servizi cloud.

Tutti i data center Microsoft Azure sono certificati secondo gli standard di sicurezza delle informazioni, riportati nella tabella sotto.

CDSA	Azure è certificato a Content Delivery e Security Assoc. Content Protection e Security standard
Certificazione CSA STAR	Azure e Intune hanno ottenuto la certificazione Cloud Security Alliance STAR con un audit indipendente
GxP	I servizi cloud Microsoft sono conformi alle Good Clinical, Laboratory, and Manufacturing Practices (GxP)
ISO 9001	Microsoft è certificata per l'implementazione di questi standard di gestione della qualità
ISO 20000-1:2011	Microsoft è certificata per l'implementazione di questi standard di gestione dei servizi
ISO 22301	Microsoft è certificata per l'implementazione di questi standard di gestione della continuità operativa
ISO 27001	Microsoft è certificata per l'implementazione di questi standard di gestione della sicurezza dei dati
ISO 27017	I servizi cloud Microsoft hanno implementato questo Codice di Procedure per i controlli di sicurezza dati
ISO 27018	Microsoft è stato il primo provider di servizi cloud a rispettare questo codice di procedure privacy
MPAA	Azure ha superato con successo una valutazione formale di Motion Picture Association of America
Certificazioni condivise	Microsoft ha dimostrato l'allineamento di Azure a questo programma tramite CSA CCM versione 3.0.1
SOC 1	I servizi cloud Microsoft sono conformi agli standard Service Organiz. Controls per la sicurezza operativa
SOC 2	I servizi cloud Microsoft sono conformi agli standard Service Organiz. Controls per la sicurezza operativa
SOC 3	I servizi cloud Microsoft sono conformi agli standard Service Organiz. Controls per la sicurezza operativa
WCAG 2.0	I servizi cloud Microsoft sono conformi alle Web Content Accessibility Guidelines 2.0

Implementazioni regionali

Microsoft Azure copre più aree geografiche di qualsiasi altro provider di servizi cloud, offrendo tutta la scalabilità necessaria per portare le applicazioni Claros agli utenti di tutto il mondo senza alterare la residenza dei dati e fornendo opzioni di conformità e resilienza esaustive per i clienti. Per consentire ai clienti di mantenere la sovranità dei dati e rispettare le normative locali, Hach utilizza i data center Microsoft Azure che si trovano nelle stesse aree geografiche dei clienti o il più vicino possibile.

50 Aree nel mondo

140 Disponibile in 140 paesi

Fonte: Microsoft

Tutti questi data center sono inoltre dotati di impianti HVAC e gruppi di continuità (UPS, Uninterruptible Power Supply) con ridondanza N+1.

Le misure di sicurezza fisica sono conformi alle best practice settoriali e includono:

- Protocolli per le schede di identificazione, protocolli di scansione biometrica, nonché sorveglianza interna ed esterna 24 ore al giorno
- Accesso consentito esclusivamente al personale autorizzato del data center (nessuno può entrare nell'area di produzione senza disporre dell'autorizzazione preventiva e di una scorta appropriata)
- Tutti i dipendenti del data center vengono sottoposti a questi controlli di sicurezza all'avanguardia

Responsabilità del cliente

Accesso controllato e configurazione degli account

Per consentire ad Hach di garantire la sicurezza dei dati, i clienti sono tenuti a rispettare gli standard di protezione richiesti. Hach impone ai clienti di verificare che ogni singolo account Claros sia configurato con i livelli di autorizzazione e accesso appropriati per ciascun utente. Ogni singolo cliente è tenuto a identificare i dipendenti dell'impianto dotati di accesso amministrativo e gestirne regolarmente gli account.

Protezione fisica

I clienti sono responsabili della protezione fisica dei propri prodotti Hach e dell'infrastruttura di sicurezza.
Ciascun impianto è responsabile per il controllo dell'accesso alla propria struttura, agli strumenti Hach utilizzati (ad esempio, controller e sensori) e alle reti di comunicazione.

Connettività

Il cliente è responsabile della connettività fra gli strumenti Hach e Claros in tutte le sue sedi. Per garantire un efficiente funzionamento di Claros, in genere è necessario collegare gli strumenti utilizzando una connessione di rete o cellulare, che deve essere gestita e adeguatamente protetta dal cliente.

DOC180.57.10159.Feb20