Hach Claros Whitepaper zur Sicherheit

Überblick

Claros ist das Water Intelligence System von Hach®. Es wurde entwickelt, um Unternehmen im Wassersektor die sichere Verarbeitung von Labor- und Prozessdaten in verwertbare Erkenntnisse zu ermöglichen und dadurch bessere Geschäftsergebnisse zu erzielen. Claros umfasst Lösungen des Hach Instrument Management, Data Management und Process Management auf einer einzigen Plattform. Hach ist sich bewusst, dass die Unterstützung beim Schutz der Daten unserer Kunden, die Gewährleistung ordnungsgemäßer Sicherheitsrichtlinien und die Minderung potenzieller Risiken von entscheidender Bedeutung sind, wenn es darum geht, Vertrauen aufzubauen und hochwertige Services bereitzustellen. Hach verfolgt einen risikobasierten Sicherheitsansatz, und in diesem Dokument werden die vielen Maßnahmen und Technologien beschrieben, die Claros zum Schutz der Daten unserer Kunden nutzt.

In diesem Dokument wird erläutert, wie Claros die grundlegenden Ziele der Informationssicherheit umsetzt: Es geht um Vertraulichkeit, Integrität und Verfügbarkeit sowie um den Ansatz von Hach im Hinblick auf die Sicherheitsarchitektur und die Verantwortlichkeiten unserer Kunden. Im Rahmen dieses Sicherheitskontexts definieren wir Vertraulichkeit als unsere Regeln, die den Zugriff auf Informationen steuern, die Integrität als Präzision und Vertrauenswürdigkeit der Informationen sowie die Verfügbarkeit als zuverlässigen Zugriff auf Informationen durch berechtigte Benutzer.

Nachfolgend finden Sie die Themen, die in diesem Dokument enthalten sind:

Der Ansatz von Hach

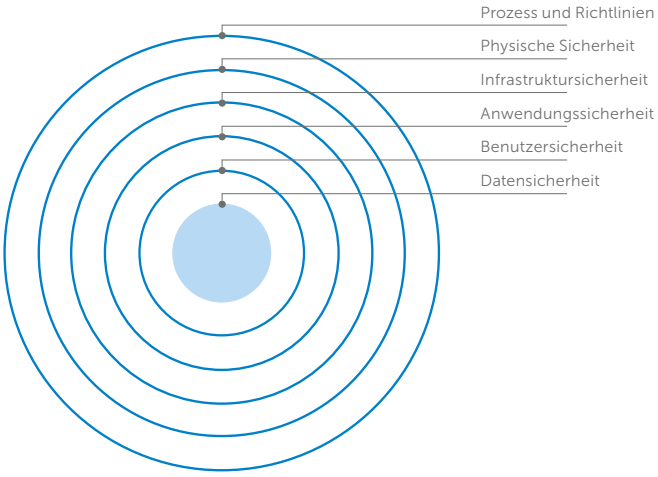
Tiefengestaffelte Sicherheit

Bei Claros gibt es nicht nur eine einzelne Ebene, die Kundendaten schützt. Es handelt sich vielmehr um eine gut durchdachte Lösung, die verschiedene Ebenen mit einbezieht – von den physischen Sicherheitsmaßnahmen im Datenzentrum bis hin zu den Zugriffsrechten, die festlegen, auf welche Daten ein einzelner Benutzer zugreifen kann. Hach nutzt diese mehrschichtige Sicherheitsstrategie zum Schutz der Kundendaten.

Die tiefengestaffelte Sicherheit ist die koordinierte Verwendung mehrerer Sicherheitsmaßnahmen, um die Integrität der Informationsressourcen in einem Unternehmen zu schützen. Die Strategie basiert auf dem militärischen Prinzip, dass es für einen Gegner schwieriger ist, ein komplexes, mehrschichtiges Sicherheitssystem zu bezwingen, als eine einzige Barriere zu durchdringen.
- TechTarget

Prozess und Richtlinien

In der ersten Sicherheitsebene geht es darum, über eine Reihe gut definierter und umfassender Sicherheitsprozesse und -richtlinien zu verfügen, um die Sicherheit der Daten unserer Kunden und unserer Anwender zu gewährleisten. Das Informationssicherheits-Managementsystem (ISMS) von Hach nutzt eine Reihe von Maßnahmen in Form von Prozessen und Richtlinien, die gewährleisten, dass die von unseren eigenen Mitarbeiter gewährleistete Sicherheit höchste Priorität hat.



Schulung

Mitarbeiter von Hach, die zum Zugriff auf Claros berechtigt sind, werden regelmäßig geschult, damit sie die unternehmensweiten Sicherheitsrichtlinien von Hach einhalten. So werden z.B. Mitarbeiter von Hach Development Operations, Research & Development sowie Technical Support and Services, die möglicherweise sensible Kundendaten und -informationen bearbeiten, regelmäßig zu den Themen Einhaltung von Richtlinien und Sicherheitsbewusstsein geschult, um die ständige Aufmerksamkeit für relevante und zu erwartende Sicherheitsbedrohungen aufrechtzuerhalten.

Autorisierter Zugriff

Zusätzlich dazu, dass nur autorisierte Mitarbeiter den Produktionsbereich betreten dürfen, ist der operative Zugriff auf Claros auf eine eingeschränkte Gruppe von Mitarbeitern von Hach Development Operations beschränkt. Der Zugriff wird über das Unternehmensnetzwerk von Hach gesteuert, sodass nur ausgewählte Mitarbeiter auf die Daten zugreifen können. Alle Mitarbeiter von Hach, die physisch oder operativ Zugriff auf Produktionsumgebungen haben, werden geschult, und alle Aktivitäten werden zur Nachvollziehbarkeit protokolliert.

Änderungskontrolle

Der formale Prozess der Änderungskontrolle von Hach minimiert die Risiken, die mit Änderungen und Aktualisierungen von Claros verbunden sind. Dieser Prozess ermöglicht die Nachverfolgung von Änderungen an Claros und überprüft, ob Risiken bewertet wurden, Abhängigkeiten untersucht werden und die erforderlichen Richtlinien und Verfahren berücksichtigt und angewendet wurden, bevor Änderungen autorisiert werden. Hach dokumentiert alle Änderungen in unseren Versionshinweisen, die im Vorfeld von Systemänderungen oder -aktualisierungen an unsere Kunden übermittelt werden.

Systemoptimierung

Claros nutzt viele gut koordinierte Technologien, um unseren Service bereitzustellen. Darüber hinaus gibt möglicherweise viele nicht benötigte Funktionen. Gemäß den Best Practices der Branche prüft Claros Development Operations die gesamte Lösung sorgfältig, um unnötige Services zu identifizieren und diese Funktionen zu entfernen und/oder zu deaktivieren, um die Anfälligkeit für Sicherheitsbedrohungen zu verringern.

Regelmäßige Anfälligkeitsprüfungen und Penetrationstests

Gemäß internen Richtlinien und internationalen Rahmenvorschriften und Standards für die Cybersicherheit führt Hach regelmäßig Anfälligkeitsprüfungen und Penetrationstests durch, die kritische Sicherheitslücken abdecken. So z.B. die OWASP Top 10, um Sicherheitsbedrohungen immer einen Schritt voraus zu sein.

Sicherheitspatches

Hach nutzt strenge Richtlinien und Verfahren, um alle Komponenten von Claros, einschließlich Betriebssysteme, VM-Hypervisoren (virtuelle Maschinen), Middleware, Datenbanken, mobile Anwendungen usw. mit den Sicherheitspatches der Anbieter zu aktualisieren. Diese Sicherheitspatch-Aktivitäten unterliegen Audits gemäß IEC 62443-4-1 „Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung" sowie strengen Standards.

Vertraulichkeit

Authentifizierung

Die Claros Architektur basiert auf einem zentralen Authentifizierungs- und Autorisierungs-Sicherheitsframework, um den Zugriff auf den Service und die Feldgeräte zu steuern. Dieses Sicherheitsframework ermöglicht die Durchsetzung von Sicherheitsrichtlinien, indem Algorithmen zur Passwortstärke zur Festlegung der Mindestlänge und -komplexität für Passwörter erforderlich sind.

Verschlüsselung beim Datenverkehr

Der gesamte ein- und ausgehende Datenverkehr von Claros wird verschlüsselt, um die Kommunikationssicherheit zu gewährleisten. Bei der Verschlüsselung wird ein TLS/SSL-Protokoll (Transport Layer Security/Secure Sockets Layer) verwendet, das entweder den SHA-2-Algorithmus (Secure Hash Algorithm 2) oder den AES-Algorithmus (Advanced Encryption Standard) nutzt. Das bedeutet, dass keine Daten, die einen der vertrauenswürdigen Endpunkte verlassen oder erreichen, unverschlüsselt sind, während sie über das Internet übertragen werden.

Verschlüsselung ruhender Daten

Hach geht keine Risiken bei ruhenden Kundendaten ein. Alle Claros Daten werden auf Microsoft Azure Servern gespeichert und mithilfe der AES-256-Bit-Verschlüsselung verschlüsselt. Selbst wenn jemand Zugriff auf die Daten auf den Servern erlangen sollte, wären sie vollständig verschlüsselt und nicht erkennbar.

Integrität

Gesteuerter und rollenbasierter Zugriff

Der gesamte Kundenzugriff auf Claros wird über Benutzeroberflächen (User Interfaces, UIs), Anwendungsprogrammierschnittstellen (Application Programming Interfaces, APIs) und/oder spezielle Tools gesteuert. Für die Verwendung einer dieser Zugriffsmethoden sind ein Benutzername und ein Passwort mit den entsprechenden Berechtigungen für den angeforderten Zugriff erforderlich. Jeder Claros Kontoadministrator kann die Berechtigungen von Benutzerkonten festlegen. Dieser Vorgang wird als rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) bezeichnet. Da die RBAC in der gesamten Claros Infrastruktur umgesetzt wird, haben Kunden keinen Root- oder administrativen Zugriff auf irgendeinen Teil der Claros Technologieplattform, und der Zugriff ist nur über die Claros Anwendungsebene (UI oder API) möglich.

Anwendungszugriff

Auf Kundendaten kann nur über die Claros Anwendung zugegriffen werden. Unabhängig davon, ob dieser Zugriff über die Benutzeroberflächen oder über verfügbare APIs erfolgt, wird die RBAC erzwungen, um den Zugriff auf die Kundendaten nur durch autorisierte Benutzer und Mitarbeiter zu regeln. Daher bietet Claros keinen direkten Zugriff auf Datenbanken. Dieser Ansatz verhindert, dass nicht autorisierte Services oder Systeme versehentlich oder böswillig Kundendaten abrufen oder ändern.

Kommunikation

Die gesamte Kommunikation mit Claros wird von den Feldgeräten initiiert, sodass Kunden alle Kommunikationsversuche von ihrem eigenen Netzwerk zur Außenwelt nachverfolgen und zusätzliche Sicherheitsmaßnahmen für das umliegende Netzwerk ergreifen können. Jeder Kommunikationsversuch mit und von Feldgeräten mit Claros wird auf seine Authentizität hin überprüft.

Firewalls

Der gesamte Netzwerkzugriff von Feldgeräten sowie auf Feldgeräte wird durch eine mehrschichtige Firewall geschützt, die im Deny-all-Modus läuft. Der Internetzugang ist nur für explizit geöffnete Ports für eine Teilgruppe der angegebenen virtuellen Hosts zulässig. Um für zusätzliche Sicherheit zu sorgen, befinden sich alle Datenbankserver hinter einer zusätzlichen Firewall.

Nicht zwingend benötigte Ports und Services

Alle Ports und Services auf allen Servern und integrierten Feldgeräten, die für den Betrieb von Claros nicht erforderlich sind, werden deaktiviert. Dadurch werden zusätzliche Möglichkeiten für Fremdeingriffe eliminiert. Nur eine Handvoll Ports und Endpunkte müssen im Netzwerk des Kunden geöffnet werden, um Claros zu nutzen. Die folgende Tabelle bietet einen Überblick über die Ports und Services, die Claros verwendet:

Port	Richtung	Service	Zweck
1194 (UDP)	Ausgang	VPN	Fernzugriff für Hach Servicetechniker ermöglichen
5671 (TCP)	Ausgang	AMQPS	Nachrichten an Claros senden und von Claros empfangen
123 (UDP)	Ausgang/Eingang	NTP	Aktuelle(s) Datum/Uhrzeit vom externen Zeitserver abrufen
80 (TCP)	Ausgang	HTTP	Gehashte und signierte Firmwareaktualisierungen aus dem Repository abrufen
443 (TCP)	Ausgang	HTTPS	Auf Claros UI zugreifen

Verfügbarkeit

Microsoft Azure

Claros nutzt Microsoft Azure Cloud-Computing für die Bereitstellung seiner Services. Daher profitieren alle Claros Kunden von der Microsoft Azure Vereinbarung zum Servicelevel (Service Level Agreement, SLA), die eine Verfügbarkeit von mindestens 99,95 % von allen wichtigen Azure Services garantiert.

Infrastruktur

Zwischen der physischen Datenzentrumsebene und der Claros Anwendungsebene befindet sich die Infrastruktur, die unsere Lösung unterstützt. In der gesamten Infrastruktur wird die Sicherheit umfassend und koordiniert implementiert, um die Sicherheit von Kundendaten zu gewährleisten.

Einhaltung von Vorschriften

Um unsere Kunden bei der Einhaltung nationaler, regionaler und branchenspezifischer Anforderungen zur Erfassung und Nutzung der Daten von Einzelpersonen zu unterstützen, bietet Microsoft Azure eines der umfassendsten Angebote an Compliance-Services aller Cloudservice-Provider nach Industriestandard.

Alle Microsoft Azure Datenzentren sind nach führenden Informationssicherheitsstandards zertifiziert, die in der folgenden Tabelle aufgeführt sind:

CDSA	Azure ist nach dem Content Delivery and Security Assoc. Content Protection and Security-Standard zertifiziert.
CSA STAR-Nachweis	Azure und Intune erhielten den STAR-Nachweis der Cloud Security Alliance auf der Grundlage eines unabhängigen Audits.
GxP	Microsoft Cloud Services halten die Gute klinische, Labor- und Herstellungspraxis (Good Clinical, Laboratory and Manufacturing Practices, GxP) ein.
ISO 9001	Microsoft ist für die Implementierung dieser Qualitätsmanagementstandards zertifiziert.
ISO 20000-1:2011	Microsoft ist für die Implementierung dieser Servicemanagementstandards zertifiziert.
ISO 22301	Microsoft ist für die Implementierung dieser Managementstandards für Geschäftskontinuität zertifiziert.
ISO 27001	Microsoft ist für die Implementierung dieser Informationssicherheits-Managementstandards zertifiziert.
ISO 27017	Microsoft Cloud Services haben diesen Leitfaden für Informationssicherheits-Kontrollmaßnahmen implementiert.
ISO 27018	Microsoft war der erste Cloud-Anbieter, der diesen Leitfaden für den Datenschutz in der Cloud befolgt hat.
MPAA	Azure hat erfolgreich eine formale Bewertung durch die Motion Picture Association of America abgeschlossen.
Gemeinsame Bewertungen	Microsoft demonstriert die Übereinstimmung von Azure mit diesem Programm durch CSA CCM Version 3.0.1.
SOC 1	Microsoft Cloud Services erfüllen die Service Organization Controls-Standards für die betriebliche Sicherheit.
SOC 2	Microsoft Cloud Services erfüllen die Service Organization Controls-Standards für die betriebliche Sicherheit.
SOC 3	Microsoft Cloud Services erfüllen die Service Organization Controls-Standards für die betriebliche Sicherheit.
WCAG 2.0	Microsoft Cloud Services erfüllen die Web Content Accessibility Guidelines 2.0.

Regionale Bereitstellungen

Microsoft Azure verfügt über mehr globale Regionen als jeder andere Cloud-Anbieter und bietet die erforderliche Skalierbarkeit, um Claros Anwendungen Benutzern auf der ganzen Welt näherzubringen. Außerdem wird die Datenresidenz bewahrt, und Kunden werden umfassende Compliance- und Flexibilitätsoptionen angeboten. Um Kunden dabei zu unterstützen, ihre Datenhoheit zu wahren und regionale Vorschriften einzuhalten, nutzt Hach Microsoft Azure Datenzentren für Kunden in ihren Regionen oder in nächster Nähe.

50 Regionen weltweit

140 Verfügbar in 140 Ländern

Quelle: Microsoft

Alle diese Datenzentren verfügen außerdem über N+1-redundante HLK-Technik und eine unterbrechungsfreie Stromversorgung (USV).

Die physische Sicherheit entspricht den Best Practices der Branche und umfasst Folgendes:

- Schlüsselkarten-Protokolle, biometrische Scanprotokolle und Rund-um-die-Uhr-Überwachung von Innen- und Außenbereichen
- Auf autorisierte Mitarbeiter im Datenzentrum beschränkter Zugriff – niemand kann den Produktionsbereich ohne vorherige Genehmigung und entsprechende Begleitperson betreten
- Jeder Mitarbeiter im Datenzentrum wird gründlichen Sicherheitsüberprüfungen unterzogen

Verantwortlichkeiten der Kunden

Kontrollierter Zugriff und Einrichtung

Damit Hach die Datensicherheit gewährleisten kann, erwarten wir auch von unseren Kunden, dass sie die Sicherheitsstandards einhalten. Hach verlässt sich darauf, dass unsere Kunden die Einrichtung jedes Claros Kontos mit den entsprechenden Berechtigungen und dem entsprechenden Zugriff für jeden Benutzer sicherstellen. Jeder Kunde muss selbst festlegen, wer in der Anlage über administrativen Zugriff verfügt, und diese Konten verwaltet.

Physischer Schutz

Die Kunden sind für den physischen Schutz ihrer Hach Geräte und der Sicherheitsinfrastruktur verantwortlich. Jeder Anwender ist selbst für den kontrollierten Zugang zur Anlage, zu relevanten Hach Geräten (z.B. Controllern und Sensoren) und Kommunikationsnetzwerken verantwortlich.

Konnektivität

Die Konnektivität der Hach Geräte mit Claros an jedem Kundenstandort liegt in der Verantwortung des Kunden. Damit Claros effektiv funktioniert, ist für die Geräte in der Regel eine Mobilfunk- oder Netzwerkverbindung erforderlich, die der Kunde aufrechterhalten und ausreichend schützen muss.

DOC180.72.10159.Feb19