HACH®
Be Right™

Water Intelligence

Security by Design, Efficiency by Nature

Claros ist Water Intelligence. Das Claros-System von Hach® kombiniert Instrument-, Data- und Processmanagement zu einer umfassenden Lösung, die auf Ihren Betrieb zugeschnitten werden kann. Claros ist auf Sicherheit ausgelegt und nutzt erstklassige Sicherheitsfunktionen, mit denen Unternehmen im Wassersektor Labor- und Prozessdaten in Erkenntnisse und Optimierungen umwandeln und gleichzeitig das Gesamtrisiko reduzieren können.

Claros basiert auf dem Konzept „Security by Design“ und auf den fünf Schlüsselprinzipien, die im Folgenden erläutert werden.

1

Mehr als eine Cloud

Hach verwendet **Microsoft Azure,** die gleiche **Cloud, auf die auch die größten Unternehmen vertrauen**, um sichere Anwendungen auszuführen und die sensibelsten Daten zu speichern. Wir haben uns für Azure entschieden, weil Microsoft es als Unternehmenslösung mit Compliance-Orientierung konzipiert hat und laut eigenen Angaben jedes Jahr durchschnittlich über 1 Mrd. US-Dollar in die Verbesserung und Aktualisierung der Sicherheit von Azure investiert. Alle Daten in Azure werden während der Speicherung und Übertragung automatisch verschlüsselt. Durch die automatische intelligente Überwachung und Profilierung des Datenverkehrs werden Bedrohungen erkannt, bevor ein Sicherheitsvorfall eintritt. Azure war die erste Cloud, die Trusted Execution Environments (TEEs) unterstützte, sodass Daten vor unbefugtem Zugriff und Manipulation geschützt werden. Es verfügt über Anti-Malware- und Virenschutzmechanismen sowie Firewalls, mit denen wir allen Claros Kunden zusätzliche Sicherheitsebenen bieten.

Hach verwendet Azure, weil wir der Meinung sind, dass Wasserversorger und Wasseraufbereitungsanlagen Schutz der Enterprise-Klasse verdienen. Laut der offiziellen Berichterstattung von Microsoft investiert Azure mehr und bietet bessere Verschlüsselung und Überwachung als IT-Teams von privaten oder öffentlichen Organisationen. Weitere Informationen zu Compliance und Zertifizierungen finden Sie im Azure Trust Center von Microsoft.

2

Best Practices der Branche

Unsere Entscheidung für die Cloud ist erst der Anfang. Da wir der Meinung sind, dass die beste Verteidigung vielschichtig ist, befolgt Hach bestimmte branchenweit bewährte **Best Practices**. Daher arbeiten wir daran, die Risiken jeglicher Angriffsmethoden zu reduzieren und sicherzustellen, dass die Daten im unwahrscheinlichen Fall eines Sicherheitsvorfalls sicher sind und wiederhergestellt werden können.

Zu diesem Zweck verfolgt Claros vier Schlüsselprinzipien:

- Alle sensiblen Daten werden in einem „Datensafe“ gespeichert, der während der Speicherung mit AES-256-Bit-Verschlüsselung und während der Übertragung mit dem Secure-Hash-Algorithmus 2 oder AES-Algorithmen verschlüsselt wird, sodass Daten selbst im Falle eines Sicherheitsvorfalls nicht mehr ausgelesen werden können.
- Unsere Systeme weisen eine Verfügbarkeit von 99,9 % für alle serverseitigen Aktivitäten auf. So wird sichergestellt, dass der Betrieb nicht durch DDoS- oder andere Angriffe, mit denen Dienststörungen ausgelöst werden sollen, beeinträchtigt wird.
- Wir erfassen regelmäßige Backup-Snapshots, damit im Falle eines kompromittierten Systems eine reibungslose und aktuelle Wiederherstellung möglich ist.
- Die Daten werden über mehrere Systeme verteilt, um einen einzelnen Ausfallpunkt zu verhindern und das Risiko einer Gefährdung zu verringern.

Mit anderen Worten: Vom Speicher bis zum Zugriff, von der Betriebszeit bis zur Wiederherstellungszeit basiert Claros auf speziellen branchenweit bewährten **Best Practices** und Zertifizierungen.

Vier Sicherheitsebenen

Verschlüsselung per Datensafe

99,9 % Serververfügbarkeit

Regelmäßige Backups

Redundante Datenverteilung

3

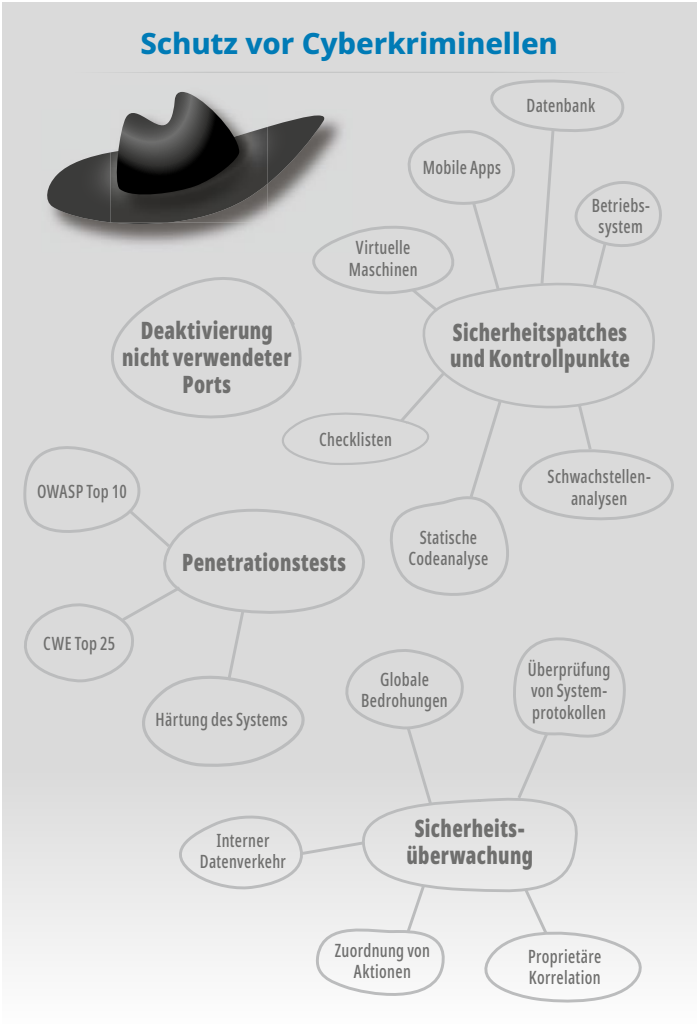
Umfassende Risikoreduzierung

Bei der Wassersicherheit ist das Risiko endemisch. Da hochwertige, komplizierte Systeme im Einsatz sind, können Fehler weitreichende Konsequenzen haben. Wie bei jedem System gibt es zwei Hauptrisikofaktoren: **Cyberkriminelle** Aktivitäten und **menschliches Versagen**. Das „Security by Design"-Konzept von Hach bietet eine umfassende Lösung für beide Faktoren.

Cyberkriminalität

Hach verwendet eine Vielzahl von Techniken, um den Zugriff durch **Cyberkriminelle** zu unterbinden und Schäden zu verhindern.

- Alle Serverports und -dienste, die für den Betrieb von Claros nicht erforderlich sind, werden deaktiviert, wodurch viele Eintrittspunkte für externe Angriffe eliminiert und die Anzahl der zu überwachenden Ports reduziert wird.
- Sicherheitspatches werden auf alle Komponenten von Claros angewendet, einschließlich des Betriebssystems, der Datenbanken, der virtuellen Maschinen und der mobilen Anwendungen. Dabei gelten strenge Richtlinien und Verfahren. Alle Softwareentwicklungen und zugehörigen Patches entsprechen den Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung gemäß IEC62443-4-1. Dieser Prozess umfasst die Ergänzung jeder Phase der Produktentwicklung um klar definierte Sicherheitsprüfpunkte und Ergebnisse, einschließlich Sicherheits-Checklisten, Schwachstellenanalysen und statischer Codeanalysen.
- Um Bedrohungen einen Schritt voraus zu sein, führt Hach häufige Tests zur Bewertung von Schwachstellen sowie Penetrationstests durch. Dazu gehören Bewertungen gemäß den OWASP Top 10, einer Liste, die den breiten Konsens über die aktuellen kritischen Sicherheitsrisiken darstellt, und gemäß den CWE Top 25, einer Liste der häufigsten Risiken und Fehler. Darüber hinaus prüft Claros Development Operations die gesamte bereitgestellte Lösung genau, um „das System zu härten", indem unnötige Dienste ermittelt und Funktionen entfernt oder deaktiviert werden, die ein erhöhtes Sicherheitsrisiko darstellen könnten.



- Hach bietet eine 360-Grad-Ansicht von Bedrohungen in Echtzeit. Das Sicherheitsüberwachungsprogramm von Hach analysiert Informationen des internen Netzwerkverkehrs, zugehörige Aktionen in Systemen und externe Informationen über Schwachstellen. Der interne Datenverkehr wird an mehreren Stellen

in unserem globalen Netzwerk auf verdächtiges Verhalten untersucht, z.B. auf das Vorhandensein von Datenverkehr, der auf Botnet-Verbindungen hinweisen könnte. Diese Analyse wird mit einer Kombination aus Open-Source- und kommerziellen Tools zur Erfassung und Analyse von Datenverkehr durchgeführt. Die Analyse wird ebenfalls von einem eigenen Korrelationssystem, das auf der Hach Technologie basiert, unterstützt. Die Netzwerkanalyse wird durch die Untersuchung von Systemprotokollen ergänzt, um ungewöhnliches Verhalten wie unerwartete Aktivitäten in Konten ehemaliger Mitarbeiter oder den versuchten Zugriff auf Kundendaten zu identifizieren.

Menschliches Versagen

Es gibt jedoch eine weitere Art von Risiko: **menschliches Versagen**. Menschliches Versagen liegt vor, wenn jemand ein Passwort auf einer Post-it-Notiz hinterlässt oder ein Passwort wählt, das sich intuitiv erraten oder mit einem Brute-Force-Angriff ermitteln lässt. Dies passiert, wenn jemand ein fremdes System benutzt und dabei über Berechtigungen verfügt, die er nicht haben sollte. Menschliches Versagen kann zu falschen Bewertungen von Daten und Maßnahmen führen, die die Effizienz verringern, oder in einigen Fällen zu Maßnahmen, die gefährliche Risiken für die Wassersicherheit darstellen können. Der Vorteil der Verwendung des Claros Water Intelligence System besteht darin, dass auch diese Fehler minimiert werden können, was zu einer umfassenderen Reduzierung des Risikoprofils führt.

Um menschliches Versagen zu reduzieren, setzt Hach zusätzliche Sicherheitsverfahren zur Ergänzung der Geräteautomatisierung und Datenerfassung ein:

- Hach verfolgt den Ansatz, den administrativen Zugriff auf jedes Hach System und alle Daten zu protokollieren. Diese Protokolle können vom Hach Sicherheitsteam nach Bedarf überprüft werden, und im Fall von Unstimmigkeiten kann ein Audit durchgeführt werden.

- Wenn Passwörter oder Passphrasen für den Zugriff erforderlich sind, setzt Hach strenge Richtlinien durch, einschließlich des Ablaufs von Passwörtern, der Beschränkung der Wiederverwendung von Passwörtern und einer angemessenen Passwortstärke. Wir verwenden die Zwei-Faktor-Authentifizierung (2FA) für den gesamten Zugriff auf Produktionsumgebungen und -ressourcen. Durch diese Maßnahmen wird das Risiko menschlichen Versagens und Phishing drastisch reduziert.
- Hach unterstützt Sie auch dabei, Sicherheitsrisiken durch strenge Genehmigungskontrollen zu reduzieren. Der operative Zugriff auf Claros ist auf eine kleine Gruppe von Hach Development Operations-Mitarbeitern beschränkt. Die Kontrolle erfolgt dabei über das Unternehmensnetzwerk, und jede Aktivität wird zur Überprüfbarkeit protokolliert, damit nichts unbemerkt geschieht.

4

Geschützt an der Quelle

Die Sicherung eines Systems erfordert die richtigen Richtlinien und Technologien. Die Zuversicht, dass ein System sicher ist, erfordert auch das Vertrauen in die Mitarbeiter, die diese Richtlinien implementieren und die Technologie bereitstellen. Hach hat viel Arbeit investiert, um dieses Vertrauen gewinnen.

Die Claros Plattform von Hach ist als ISO-27001-konform zertifiziert; ein weithin bekannter Normensatz für die Verwaltung sensibler Daten und die Entwicklung von Anwendungen in einer sicheren Umgebung. Mitarbeiter von Hach, die zum Zugriff auf Claros berechtigt sind, werden regelmäßig geschult, damit sie die unternehmensweiten Sicherheitsrichtlinien von Hach einhalten. Dazu gehören technische Support- und Servicemitarbeiter sowie Mitarbeiter aus dem Bereich Betrieb und alle Personen, die mit sensiblen Kundendaten und -informationen arbeiten können. Die Schulungsthemen umfassen Compliance, sichere Codierung und Sicherheitsbewusstsein. So werden alle Mitarbeiter über relevante und neue Bedrohungen informiert, bevor sie zu einem Problem werden. Hach betreibt außerdem eine DevOps-Abteilung, die für den Betrieb und die Wartung von Claros zuständig ist.

Zertifizierungsprozess

1. Vorläufiges Audit
Inventarisierung einschließlich Dokumentprüfung zur Überprüfung der Vollständigkeit und Einhaltung von Normen.

2. Zertifizierungsaudit
Phase 1: Prüfung der ISMS-Dokumentation
Phase 2: Bestätigung der ISMS-Wirksamkeit

3. Berichterstattung
Audit-Dokumentation einschließlich Bewertung des Managementsystems

4. Zertifizierung
Nachweis der erfolgreichen Zertifizierung mit einer maximalen Gültigkeitsdauer von 3 Jahren

NACH 1 JAHR

5. Erstes Überwachungsaudit
Prüfung der ISMS-Implementierung

NACH 2 JAHREN

6. Zweites Überwachungsaudit
Wiederholte Prüfung der ISMS-Implementierung

7. Rezertifizierung
Wiederholung der Schritte 3 bis 7 für Verlängerung um weitere 3 Jahre

5

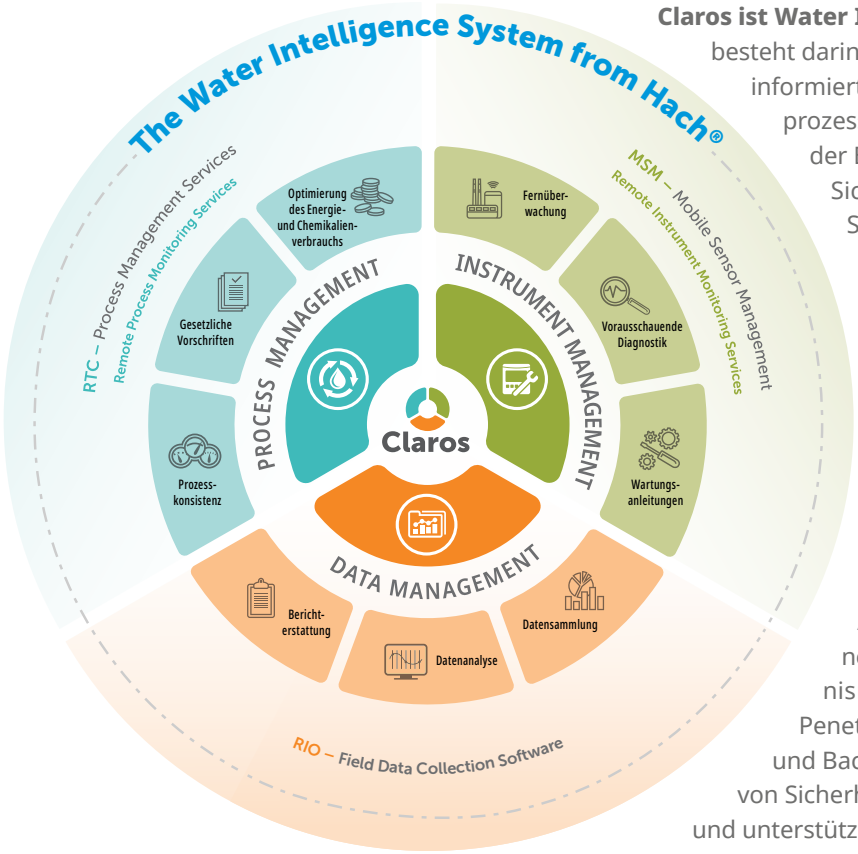
Datenschutz und Einhaltung gesetzlicher Vorschriften

Hach hat sich einem einfachen Prinzip verpflichtet: Ihre Daten sind Ihre Daten. Claros erfasst nur Daten, die für die Claros-Plattform relevant sind – z.B. Messdaten, Parameter und Geräte-IDs –, sowie Informationen, die für eine effektive Kommunikation und Koordination erforderlich sind, einschließlich Name der Anlage, E-Mail-Adresse des Kunden und Benutzernamen. Die Daten bleiben Eigentum des jeweiligen Kunden, und Hach verkauft niemals personenbezogene Daten oder Kundendaten an Dritte. Dies gewährleisten wir durch jährliche Compliance-Bewertungen gemäß der Datenschutz-Grundverordnung (DSGVO).

Hach verfolgt den Ansatz, dass Ihre Daten Ihnen gehören, sodass Sie die Daten nutzen und Ihre Anlage zuversichtlich betreiben können.

Ein großer Teil dieses Sicherheitssystems ist Compliance. Hach hat neben den strengen Sicherheitsverfahren, wie oben im Abschnitt zur Drittanbieter-Zertifizierung beschrieben, verschiedene Entscheidungen umgesetzt, damit Compliance und Sicherheit Hand in Hand gehen. Einer der Vorteile von Azure besteht beispielsweise darin, dass die Server in 140 Ländern verfügbar sind. Damit kann Hach weltweit mehr Kunden bedienen und sicherstellen, dass die Kunden nationale Richtlinien zum Standort gespeicherter Daten einhalten können.

Sicherer und intelligenter mit „Security by Design“



Claros ist Water Intelligence, und Teil eines intelligenten Konzepts besteht darin, Sicherheit zu gewährleisten, über Bedrohungen informiert zu werden, diese Bedrohungen in den Entwicklungsprozess zu integrieren, eine Cloud-Umgebung mit Sicherheit der Enterprise-Klasse zu wählen, robuste, mehrstufige Sicherheitsframeworks einzurichten und die internen Sicherheitsteams zu schulen, um bei jedem Schritt die Sicherheit von Kunden, kritischen Daten und Produkten zu gewährleisten.

Mit **Security by Design** meinen wir die Implementierung von Best Practices und Sicherheitsverfahren, die dazu beitragen, sowohl das allgegenwärtige Risiko, das von Cyberkriminellen ausgeht, als auch menschliches Versagen, das einem Kunden sonst entgehen könnte, zu verringern. Ebenso geht es um die Weiterentwicklung von Sicherheitsprotokollen: Aktualisierung von Tests auf Sicherheitslücken bei neuen Bedrohungen, Entwicklung von Schutzmechanismen für das Umkreisnetzwerk, regelmäßige Penetrationstests und bessere administrative Kontrollen und Backups. Doch auch das Bereitstellen eines Teams von Sicherheitsexperten zählt dazu. Diese beraten die Kunden und unterstützen sie dabei, sichere Ergebnisse zu erzielen und das Gesamtrisiko zu reduzieren.

Denn **Security by Design ermöglicht Efficiency by Nature**. Unsere Kunden verbessern die weltweite Wasserversorgung, indem sie sauberes Wasser für Trinkwasser, Produktion und mehr ermöglichen. Sie verdienen die Effizienz und Überwachung, mit der sie ihre Arbeit erleichtern, den Chemikalienbedarf reduzieren und optimale Ergebnisse erzielen können. Wir halten uns an Best Practices für die Sicherheit, damit unsere Kunden sich mit Zuversicht auf ihr Geschäft konzentrieren können.

Das ist Water Intelligence.
Das ist Claros.

HACH®

DOC063.72.30755.Sep22