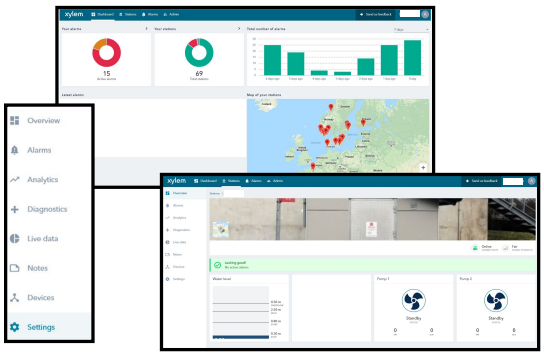
DATENSCHUTZ- UND DATENSICHERHEITSRICHTLINIE

90027103_2.0



Avensor™

1 Cybersicherheit bei Xylem

Die Cybersicherheit eines Produkts ist heutzutage eine Forderung des Marktes, um das Vertrauen unserer Kunden zu gewinnen. Xylem nimmt diese Forderung ernst und möchte das Vertrauen erhöhen, das die Kunden in unsere Produkte und unseren Service setzen. Unsere Kunden habne ihre Sorgen bezüglich der Sicherheit eines zunehmend vernetzten und cloudbasierten Lösungspakets klar zum Ausdruck gebracht. Das Cybersecurity-Team von Xylem kann die IT-Abteilungen unserer Kunden dabei unterstützen, die Leistung des Analyse- und Leistungsmanagements zu maximieren. Wir halten während des gesamten Prozesses die strengsten Sicherheitsstandards ein.

2 Datenschutz

Xylem befolgt eine interne Datenschutzrichtlinie, welche die Bestandteile der EU-Datenschutzgrundverordnung (DSGVO) umfasst. Ähnlich wie bei der DSGVO soll die Datenschutzrichtlinie von Xylem unseren Kunden helfen, folgenden Punkte zu verstehen:

- Welche Daten Xylem erhebt
- Wie Xylem die Daten verwendet
- Die Maßnahmen, mit denen Xylem die Daten schützt
- Die Rechte gemäß den geltenden Gesetzen

Lesen Sie für weitere Informationen zur Datenschutzrichtlinie *Weitere Informationen* auf Seite 2.

3 Datensicherheit

Xylem legt höchsten Wert auf die Verfügbarkeit, Integrität und Vertraulichkeit aller Leistungen, die wir unseren Kunden anbieten. Die Sicherheit dieser Produkte und Services unterliegt dem Xylem-Produktprogramm für Cybersicherheit.

4 Das Xylem-Produktprogramm für Cybersicherheit

Unsere Mission ist es, Innovationen und die besten Services der Branche in die weltweite Wasserwirtschaft einzuführen. Daher hat Xylem ein Produktsicherheitsprogramm eingeführt, das auf die Branche und das Modell der drei Verteidigungslinien ausgerichtet ist.

Erste Verteidigungslinie

Jede Geschäftseinheit bei Xylem verfügt über ein spezielles Sicherheitsteam, das die entsprechenden Produktlinien unterstützt. Diese Teams haben die folgenden Funktionen:

- Für die Sicherheit der Produkte sorgen
- Auf Schwachstellen und Vorfälle reagieren
- Mit den Kunden zusammenarbeiten, um ein hohes Absicherungsniveau zu gewährleisten

Diese Teams sind außerdem in ihrer Größe angepasst, um die Größe des jeweiligen Produktportfolios widerzuspiegeln.

Zweite Verteidigungslinie

Das globale Produktsicherheitsteam hat die folgenden Aufgaben:

- Die Risiken über das gesamte Xylem-Produktportfolio überwachen
- Als Eskalationspunkt bei Problemen agieren
- Als einheitliche Stimme von Xylem zum Thema Produktsicherheit agieren

Dieses globale Team stellt verschiedene Services zur Verfügung, an deren Spitze Experten im Unternehmensteam stehen und die im Wesentlichen von gewerblichen Sicherheitspartnern ausgeführt werden. Diese Organisation erzeugt Skaleneffekte für die einzelnen Geschäftsbereiche. Diese Services sind entscheidend:

- Das Response-Team bei Produktsicherheitsvorfällen überwacht Schwachstellen im industriellen Raum und in unserer Lieferkette. Es ist bereit, den Kunden über Cybersicherheitsvorfälle zu berichten, die unsere Produkte betreffen.
- Die gemeinsamen Serviceleistungen sorgen dafür, dass die Software auf den Technologieplattformen sicher ist und die neuen Normen in der Branche erfüllt.

Da sie diese Services anbieten, können sich die Produktsicherheitsteams auf ihre Kernkompetenz konzentrieren – als Produktexperten und beratende Partner für die Ingenieure zu agieren.

Dritte Verteidigungslinie

Das Interne Prüfungsteam bei Xylem prüft die Geschäftsbereiche regelmäßig, um die allgemeine Wirksamkeit des Programms zu gewährleisten. Die Qualität und Effektivität des Programms ist sowohl für den Xylem-Vorstand als auch für das interne Kommitee für Cybersicherheit von Bedeutung.

Das Kommitee für Cybersicherheit erhält monatliche Metriken. Aus diesen Metriken werden die stetigen internen Bemühungen ersichtlich, die Sicherheit der Xylem-Produkte in Entwicklung genauso wie der Produkte im Einsatz zu verbessern.

5 Avensor™

Avensor™ nutzt die Cloud-Plattform Xylem, eine intelligente Infrastruktur, welche die Verarbeitung, Umwandlung und Analyse von Sensordaten ermöglicht. Wenn Avensor™ mit der Cloud-Plattform Xylem kombiniert wird, richtet es sich an der Xylem-Produktsicherheitsplattform aus. Mit dem Programm können die einzelnen Plattformen aktiviert werden, sodass unsere Kunden wertvolle Einblicke gewinnen und datengestützte Entscheidungen sicher treffen können.

Implementierung

Avensor™ und die Cloud-Plattform Xylem werden auf den Amazon World Services (AWS) implementiert und in Datenzentren mit hoher Verfügbarkeit ausgeführt. Dies schließt alle Daten ein, beispielsweise auch Backups. Die Standorte werden stetig bewertet und entsprechend den Bedürfnissen unserer Kunden sowie der geltenden Compliance-Anforderungen angepasst.

6 Zugriff und Steuerung der Datenzentren

Cloud-Sicherheitsumgebung

Xylem unterstützt die Verwendung erstklassiger Partner im Cloud-Computing, um die Skalierbarkeit zu fördern und die Sicherheitsvorkehrungen zu verbessern. Zusammen mit AWS arbeiten wir in einem Modell gemeinschaftlicher Haftung, in dem sich alle Teilnehmer auf ihre Stärken konzentrieren könnnen.

Die gemeinsamen Verantwortlichkeiten werden folgendermaßen aufgeteilt:

- AWS ist für die Sicherheit der Cloud verantwortlich, einschließlich der Sicherheit der AWS-Datenzentren. Weitere Informationen entnehmen Sie bitte *Weitere Informationen* auf Seite 2.
- Xylem ist für die Sicherheit innerhalb der Cloud verantwortlich. Wir verwenden die Methoden und Ressourcen, die AWS bereitstellt, um die sichere Einrichtung unserer Anwendungen zu gewährleisten und den korrekten Datenzugriff zu definieren.

Ähnliche Aspekte umfassen:

- Schutz gegen Verteilte Dienstverweigerungs- (DDoS)-Angriffe auf Netzwerkebene
- Eine Webanwendungs-Firewall (WAF) als Schutz gegen Bedrohungen auf Anwendungsebene
- Private Netzwerke, um ausgewählte Datenströme vom öffentlichen Internet zu isolieren
- Remote-Dienstverwaltung über Virtuelle Private Netzwerke (VPN)
- Multi-Faktor-Authentifizierung (MFA) für die Cloud-Verwaltung und die rollenbasierte Zugriffssteuerung
- Branchenübliche Verschlüsselung der Daten während der Übertragung und der Daten in Ruhe, beispielsweise TLS, VPN und AES
- Stetige Sicherheitsprotokollierung und -überwachung
- Mehrfach hochgradig verfügbare (HA) Serviceinstanzen, die über mehrere Zonen implementiert werden

Produktsicherheit

Der Software-Entwicklungslebenszyklus (SDLC) umfasst Aktivitäten, die eine sichere und zuverlässige Produktentwicklung gewährleisten.

Ähnliche Aspekte umfassen:

- Das Sicherheits-Framework auf Grundlage bewährter Praktiken, beispielsweise der Xylem-Richtlinie und der IEC 62443-Norm.
- Bedrohungsmodellierung und Risikoprofilerstellung, um Sicherheitsrisiken zu erkennen
- Architekturprüfungen, die erkannte Risiken bearbeiten sowie Design für Sicherheitserwägungen
- Sicherheitsbewusstsein, um die Entwicklungsbemühungen zu unterstützen, beispielsweise sichere Code-Techniken
- Eine automatische und manuelle Sicherheitsprüfung, um Sicherheitslücken zu überprüfen und zu erkennen
- Enge Zusammenarbeit mit dem Produktsicherheitsteam

7 Weitere Informationen

- Weitere Informationen zum Xylem-Produkt-Cybersicherheitsprogramm und den Kontakt zu unserem Sicherheitsteam finden Sie unter xylem.com/security.
- Weitere Informationen zu den AWS-Sicherheitspraktiken finden Sie unter https://aws.amazon.com/compliance/shared-responsibility-model/.
- Weitere Informationen zur Xylem-Datenschutzrichtlinie finden Sie unter https://www.xylem.com/en-us/support/privacy/.

Xylem Water Solutions Global Services AB 556782-9253
361 80 Emmaboda
Sweden
Tel: +46-471-24 70 00
Fax: +46-471-24 74 01
http://tpi.xyleminc.com

90027103_2.0_de-DE_2021-03_GSI_Avensor™

xylem
Let's Solve Water